SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

Mislav Matusina

Zaštita osobnih podataka s osvrtom na Opću uredbu o zaštiti podataka

DIPLOMSKI RAD

Zagreb, Rujan 2017.

SVEUČILIŠTE U ZAGREBU

FAKULTET PROMETNIH ZNANOSTI

DIPLOMSKI RAD

Zaštita osobnih podataka s osvrtom na Opću uredbu o zaštiti podataka

Mentor:

doc. dr. sc. Goran Vojković

Student:

Mislav Matusina, univ. bacc.ing. traff

JMBAG :0135216602

Zagreb, Rujan 2017.

Sažetak/summary i ključne riječi/keywords

Zaštita osobnih podataka s osvrtom na Opću uredbu o zaštiti podataka

SAŽETAK

Pristupanjem Republike Hrvatske Europskoj uniji 1. srpnja 2013., Vlada Republike Hrvatske obavezna je primijeniti sve propise koje izdaju nadležne institucije Europske unije, pa tako i na primjenu uredbi o zaštiti osobnih podataka.

Zemlje članice Europske unije prolazi kroz mnogobrojne promjene tijekom perioda koji su odredile njene nadležne institucije, a odnose se na obavezu povećanja sigurnosti i zaštite osobnih podataka na razini cijele unije. Nova uredba se odnosi na sve radnje koje se vrše nad osobnim podatcima, uključujući prikupljanje podataka, obradu i prenošenje podataka unutar država članica Europske unije.

KLJUČNE RIJEČI: uredba; zakon o zaštiti osobnih podataka; regulativa, opća uredba o zaštiti osobnih podataka

Personal data protection with review to General Data Protection Regulation

Summary

With the accession of the Republic of Croatia to the European Union on 1 July 2013, the Government of the Republic of Croatia is obliged to apply all the regulations issued by the competent institutions of the European Union, and also to the application of the Personal Data Protection Regulation.

The EU member states is going through a number of changes over the period that is specified by its competent institutions, which refer to the obligation to increase the security and protection of personal data at the all EU countries. The new regulation refers to all actions taken over personal data, including data collection, processing and transfer of data between EU Member States.

KEYWORDS: Regulation; law on the protection of personal dana, General Data Protection Regulation, GDPR

SADRŽAJ

1. Uvod

Ovaj diplomski rad daje pregled zakona, uredbi i direktiva koje se odnose na zaštitu osobnih podataka u Republici Hrvatskoj i svim ostalim zemljama Europske unije. Pojavom interneta i povećanja usluga koje pružaju telekom operatori ostvaruje se veliki prihod pri kojem dolazi do česte izmijene osobnih podataka između korisnika i operatora. Svaka firma ili obrt ima neku određenu bazu podataka u kojoj se nalaze podatci o kupcima, korisnicima ili klijentima. Zbog raznih prodaja podataka, industrijske špijunaže i slično došlo je do donošenja novih propisa kako bi se zaštitili osobni podatci pojedinaca i njihovi životi. Do nedavno se koristila stara Direktiva o zaštiti osobnih podataka koja se nije mijenjala gotovo 20 godina. U tom periodu je tehnologija uvelike napredovala te se pojavila i veća opasnost od krađe osobnih podataka a uz to i veća potreba za zaštitu istih. Veliki broj korisnika koristi društvene mreže koje imaju trend stalnog porasta broja korisnika. Korisnici istih mreža nisu upoznati sa zaštitom osobnih podataka niti znaju koje su potencijalne opasnosti, stoga bez razmišljanja objavljuju svoje privatne slike, račune, mjesta na koja izlaze pa čak i slike osobnih iskaznica, na taj način ugrožavaju svoje društveno i ekonomsko stanje. Nije jedini način ugrožavanja vlastite sigurnosti samo putem društvenih mreža, velika opasnost se danas pojavljuje i putem online kupovine i kupovine putem telefona. Zbog povećanih obaveza ljudi i manjka slobodnog vremena sve veći broj korisnika kupuje putem spomenutih kanala. Prilikom kupovine putem interneta prodavatelju je potrebno dati vlastite osobne podatke koji su potrebni da bi se mogla dostaviti narudžba na adresu kupca, pritom malo kupaca razmišlja da potpunom neznancu daje osobne podatke koju su najčešće ime, prezime, adresa, mail pa čak i broj kreditne kartice. Dobivanjem spomenutih podataka snalažljiva osoba može lako doći do raznih lozinki te preuzeti cjelokupan identitet osobe čiji su podatci.

Cilj ovog diplomskog rada je na odgovarajući način analizirati i predstaviti osnovne pojmove koji se vežu uz osobne podatke i novu Uredbu o zaštiti osobnih podataka koja je donesena 2016. godine. Kroz rad će biti uspoređene prijašnje uredbe, sadašnje uredbe i razlozi uvođenja nove uredbe.

Iz navedenog se može zaključiti kako je vrlo potrebno pokrenuti rješavanje pitanja vezanih za zaštitu osobnih podataka te pokrenuti svijest cjelokupnog stanovništva kako bi svi više pazili na svoje podatke.

Ovaj diplomski rad je sastavljen od 8 poglavlja prema sljedećem slijedu:

1. Uvod
2. Važnost zaštite osobnih podataka
3. Postojeća (dosadašnja) pravna regulativa
4. Razlozi potrebe donošenja novih propisa
5. Opća uredba o zaštiti podataka – UREDBA (EU) 2016/679
6. Primjena Opće Uredbe u praksi
7. Dionici primjene – poznavanje (anketa)
8. Zaključak

Drugo poglavlje ovog diplomskog rada daje pregled zakona o zaštiti podataka, predstavlja neke osnovne pojmove kao što je osobni podatak. Važnost zaštite osobnih podataka je podijeljena u dvije skupine, važnost zaštite podataka u realnom svijetu i važnost zaštite podataka u virtualnom svijetu. U ovom poglavlju također će biti govora o tehnikama prikupljanja podataka te potencijalnoj opasnosti od krađe identiteta.

Treće poglavlje se sastoji od četiri potpoglavlja od kojih prvo potpoglavlje donosi pregled Konvencije 108 Vijeća Europe za zaštitu osobni podataka glede automatske obrade podataka. Drugo potpoglavlje prikazuje dosadašnju Direktivu 95/46/EZ koja se koristila gotovo dva desetljeća. U trećem potpoglavlju bit će govora o Direktivi 2002/58/EZ Europskog parlamenta i Vijeća gdje su donesena pravila o zaštiti podataka u području elektroničkih komunikacija. Spomenuta Direktiva se još naziva Direktiva o privatnosti i elektroničkim komunikacijama. Četvrto potpoglavlja će nam približiti Agenciju za zaštitu osobnih podataka poznatu pod kraticom AZOP.

Četvrto poglavlje navodi razloge potreba donošenja novih propisa. Neki od razloga su tehnička i tehnološka unaprjeđenja. Biti će govora o procesorskoj moći

nekada i danas, te o nekadašnjim super računalima od nekoliko tona, pa do modernih čipova koji imaju veću snagu nego nekadašnja računala koja su zauzimala cijele zgrade. Također, bit će govora i prikupljanju podataka i njihovoj obradi putem identifikacijske tehnologije. U jednom potpoglavlju obradit će se tema obrade i prikupljanja prometnih podataka a u zadnjem potpoglavlju bit će govora o obradi i prikupljanju podataka o lokaciji.

U petom poglavlju glavnog govora će biti o novoj Općoj uredbi o zaštiti osobnih podataka, radi se o Uredbi (EU) 2016/679. spominjat će se neki od članka, te iznosi kazni u slučaju da netko prekrši propise.

Šesto poglavlje donosi pregled primjene Opće uredbe u praksi. Biti će nekoliko citata sa FSEC simpozija o sigurnosti, koji je održan u Varaždinskom HNK 7.9.2017. godine.

Sedmo poglavlje se sastoji od dva potpoglavlja. Prvo potpoglavlje osmog poglavlja opisuje potrebu za provođenjem anketnog upitnika kako bi se ispitala svijest različitih skupina ljudi o postojećim promjenama koje se događaju na području zaštite osobnih podataka u EU zemljama.

Zadnje poglavlje daje zaključak koji proizlazi iz razrade tematike rada kroz nekoliko ključnih misli kojima se iskazuje smisao cijelog procesa koji je započeo mijenjati zakone važne za privatnost i zaštitu stanovnika Europske unije.

2. Važnost zaštite osobnih podataka

Temeljna prava svakog čovjeka na svijetu su poštivanje njegovog privatnog života i zaštita osobnih podataka. Zaštitom osobnih prava jamči se privatnost osobe u današnjem digitalnom dobu te jača sigurnost te osobe i njegova ljudska prava. Osobnim podatkom možemo smatrati svaku informaciju koja se odnosi na identificiranu osobu ili osobu koja se može identificirati. Političke korijene ljudskih prava nalazimo već u Velikoj povelji[1], kojom se građanima priznaju određena prava koja su kralju ograničila vlast. [15]

Svaka osoba se može identificirati po nekom obilježju. U Hrvatskoj su se nekada osobe u službenim ustanovama identificirale po JMBG-u (jedinstveni matični broj građana), ukoliko bi netko saznao JMBG određene osobe mogao bi iz njega očitati, datum i mjesto rođenja te spol vlasnika JMBG. Prije nekoliko godina uveden je novi identifikacijski broj koji se naziva OIB (Osobni Identifikacijski Broj), dodjeljuje se računano bez odavanja osobnih podataka o korisniku, kao što su datum i godina rođenja, spol ili mjesto rođenja.

Osim po OIB-u osobe se mogu identificirati prema fizičkom, mentalnom, psihološkom, gospodarskom, kulturnom ili socijalnom identitetu. Osobni podatak može biti adresa e-pošte, telefonski broj, broj kartice bankovnog računa ili privatna fotografija. Osobni podatak čak može biti sindikalno članstvo, odabir političke stranke, mjesečna financijska primanja osobe, zdravstveno stanje i spolni život. Podatci o kaznenom i prekršajnom postupku također mogu biti osobni podatci koji su drugačije klasificirani te se zbog toga moraju dodatno čuvati, odnosno potrebno im je osigurati posebnu zaštitu.

Da bi mogli vršiti bilo kakvu identifikaciju potrebno je prvo prikupiti podatke te ih obraditi. Obradom osobnih podataka smatra se svaka radnja ili skup radnji na osobnim podatcima. Radnje koje obično povezujemo s osobnim podatcima su prikupljanje,

[1] Poznata još i kao Magna Charta Libertatum, potpisana od strane engleskog kralja

snimanje, organiziranje, spremanje, prilagodba ili izmjena, povlačenje, uvid, svrstavanje ili kombiniranje, brisanje, arhiviranje, uništavanje, te provedba matematičkih operacija nad njima. [1][2]

2.1. Zakon o zaštiti podataka

Privatnost se pojavljuje kao pojam u svim kulturama još od davnina tako se oko 200. godine u Zborniku židovskih zakona štiti osoba od tuđeg zavirivanja u svoju kuću.[17] Privatnost se može definirati na razne načine ovisno o vremenu, sredini, okruženju i kontekstu u kojem se tim pojmom koristi. Prema A. F. Westinu privatnost je želja ljudi da slobodno biraju pod kojim uvjetima i u kojoj mjeri će izložiti sebe, svoje stavove i svoje ponašanje drugima, a dok je za J. Michaela privatnost pravo pojedinca da bude zaštićen od nedopuštenog zadiranja u njegov osobni život ili posao, ili njegove obitelji, neposrednim fizičkim mjerama ili objavljivanjem informacija.[17] [38]

Zaštita podataka se može odnositi na privatne i na pravne osobe. U Hrvatskoj je svakoj osobi zagarantirana zaštita osobnih podataka bez obzira na spol, rasu, vjeru ili državljanstvo. U zakonu o zaštiti osobnih podataka spominje se veliki broj izraza. Česti izrazi u zakonu su osobni podatak, obrada osobnih podataka, zbirka osobnih podataka, voditelj zbirke osobnih podataka, treća strana, primatelj, izvršitelj obrade, privola ispitanika, službenik za zaštitu osobnih podataka. Svi navedeni pojmovi jasno su objašnjeni u Zakonu o zaštiti podataka (ZOP.) Pročišćeni tekst Zakona o zaštiti osobnih podataka obuhvaća (»Narodne novine«, br. 103/03.), Zakon o dopunama Zakona o zaštiti osobnih podataka (»Narodne novine«, br. 118/06.), Zakon o izmjenama i dopunama Zakona o zaštiti osobnih podataka (»Narodne novine«, br. 41/08.) i Zakon o izmjenama i dopunama Zakona o zaštiti osobnih podataka (»Narodne novine«, br. 130/11.) u kojima je utvrđeno vrijeme njihova stupanja na snagu. [3] [8]

1. „*Osobni podatak je svaka informacija koja se odnosi na neku identificiranu fizičku osobu ili fizičku osobu koja se može identificirati…*“
2. *“Obrada osobnih podataka je svaka radnja ili skup radnji izvršenih na osobnim podatcima, bilo automatskim sredstvima ili ne, kao što je prikupljanje, snimanje, organiziranje, spremanje, prilagodba ili izmjena, povlačenje, uvid, korištenje, otkrivanje putem prijenosa, objavljivanje ili na drugi način učinjenih dostupnim, svrstavanje ili kombiniranje, blokiranje, brisanje ili uništavanje , te provedba logičkih, matematičkih i drugih operacija s tim podatcima.“*
3. *„Zbirka osobnih podataka je svaki strukturirani skup osobnih podataka koji je dostupan prema posebnim kriterijima, bilo centraliziranim, decentraliziranim ili raspršenim na funkcionalnom ili zemljopisnom temelju i bez obzira na to da li*

je sadržan u računalnim bazama osobnih podataka ili se vodi promjenom drugih tehničkih pomagala ili ručno.“

4. *„Voditelj zbirke osobnih podataka je fizička ili pravna osoba, državno ili drugo tijelo koje utvrđuje svrhu i način obrade osobnih podataka, kada je svrha i način obrade propisan zakonom, istim sa zakonom određuje i voditelj zbirke osobnih podataka.“*
5. *„Treća strana je fizička ili pravna osoba, državno ili drugo tijelo, osim ispitanika, voditelja zbirke osobnih podataka ili izvršitelja obrade osobnih podataka i osoba koje voditelj zbirke ili izvršitelj obrade izravno ovlasti na obradu osobnih podataka.“*
6. *„Primatelj je fizička ili pravna osoba, državno tijelo ili drugo tijelo kojem se osobni podatci otkrivaju, neovisno o tome je li on ujedno i treća strana ili nije. Međutim, državna tijela koja mogu primati podatke u okviru provođenja istrage ne smatraju se primateljima.“*
7. *„Izvršitelj obrade je fizička ili pravna osoba, državno ili drugo tijelo, koje obrađuje osobne podatke u ime voditelja zbirke osobnih podataka.“*
8. *„Privola ispitanika je slobodno dano i izričito očitovanje volje ispitanika kojom on izražava svoju suglasnost s obradom njegovih osobnih podataka u odrađene svrhe.“*
9. *„Službenik za zaštitu osobnih podataka je osoba imenovana od stane voditelja zbirke osobnih podataka koja vodi brigu o zakonitosti obrade osobnih podataka i ostvarivanju prava na zaštitu osobnih podataka.“* [3]

2.2. Važnost zaštite podataka u realnom svijetu

Važnost zaštite osobnih podataka se najbolje može prikazati na primjeru krađe identiteta gdje neka osoba ili skupina osoba mogu oštećenoj osobi nanijeti materijalnu ili neku drugu štetu. Danas se u medijima puno govori zlouporabi tuđih podataka, kao česti primjer navodi se produljivanje ugovora kod telekom operatera i nanošenja materijalne štete oštećenoj osobi. Ukoliko se dogodi situacija da netko pronađe ili ukrade osobnu iskaznicu osobe koja je korisnik usluga nekog operatera, osoba koja posjeduje tuđu osobnu iskaznicu dolazi do osobnih podataka korisnika. Posjedovanjem broja osobne iskaznice moguće je doći do OIB-a te osobe. Osoba koja se lažno predstavlja može putem osobnih podataka oštećenog korisnika putem telefonske narudžbe upiti mobilni uređaj i produljiti ugovor bez da pravi vlasnik to i sazna. Pri razgovoru da korisnikom većina agenata u pozivnom centru vrši identifikaciju po OIB-u ili po broju osobne iskaznice. Agent pozivnog centra uz dobivene točne informacije i pročitane sve osobne podatke ne može ni na koji način

znati da se ne radi o osobi o kojoj je riječ. Da bi se takve prevare spriječile svaki iskusniji agent već po zahtjevima osobe koja zove može procijenit radi li se o prevari. Najočitiji primjer takve krađe identiteta događa se kada osoba koja zove telefonom naruči nekoliko novih brojeva na najjačim tarifama te uz to i nove mobilne uređaje visoke vrijednosti. Osoba koja s lošom namjerom prikuplja nečije podatke najčešće te podatke koristi u svrhu obrade podataka ili u konačni za zlouporabu i lažno predstavljanje.

2.2.1. Tehnika prikupljanja povjerljivih podataka u realnom svijetu

Osoba koja ima u cilju izvršiti prevaru može na vrlo jednostavan način doći do osobnih podataka. Jedna od najučinkovitijih tehnika za prikupljanje osobnih podataka je socijalni inženjering koji se temelji na ljudskim greškama, odnosno ljudskom faktoru. Ovom tehnikom osoba može bez direktnog pokušaja upada informacijski sustav neke kompanije doći do osobnih podataka manipulacijom ljudstva. Informacije se prikupljaju koristeći ljudske osobine kao što su povjerenje, znatiželja, strah od nepoznatog, strah od gubitka i nemarnost. Cilj socijalnog inženjeringa u realnom svijetu je izvođenje prevara pomoću isprava oštećene osobe kako bi se nanijela novčana šteta toj osobi. Nezadovoljni radnici, bivši radnici i špijuni mogu dati podatke u krive ruke s ciljem industrijske špijunaže kako bi se ostvarila konkurentnost na tržištu i slično. Primjer ovakvog napada je lažno predstavljanje i dolazak na radno mjesto žrtve glumeći zaposlenog ili čak vanjskog suradnika, čistačicu ili slično, tada napadač može prekopavanjem smeća, pregledavanjem papira po stolu doći do nekih tajnih informacija koje može iskoristiti protiv žrtve.

Društveni inženjering[2] - obuhvaća brojne i raznovrsne načine pribavljanja lozinki za neovlašten pristup sustavu:

[2] U literaturi se često spominje pod nazivima eng. Human engineering, Social engineering

- Shoulder Surfing je tehnika otkrivanja lozinka neposrednim fizičkim uvidom prilikom upisa lozinke a da žrtva napada toga nije ni svjesna
- Strvinarenje[3] je tehnika kopanja po smeću, pretraživanjem bačenih papira ili pregleda tuđih bilješki kako bi se našla tajna lozinka za ulazak u sustav ili bilo koji drugi podatci koji se mogu iskoristiti pri neovlaštenom pristupu nekom računalnom sustavu, ovlaštene osobe svojom nepažnjom mogu dati svoju lozinku na uvid napadaču na način da se ne odjavi ili ne zaključa svoje računalo prilikom odlaska na pauzu ili prilikom zatvaranja svoga radnog mjesta u tom trenutku napadač može nastaviti koristiti računalo
- Maskiranje ili varanje[4] je metoda lažnog predstavljanja, preuzimanja identiteta druge osobe ili uloge nekog drugog računalnog sustava, u takve načine spada lažno predstavljanje npr. putem telefona kao da je u pitanju ovlašteni serviser kako bi se iskoristila naivnost i nepažnja žrtve i kako bi se došlo do lozinke ili telefonskog broja za daljinski pristup sustavu, još jedna i ne tako rijetka metoda naziva se zloupotreba povjerenja[5] gdje se postiže neovlašten pristup sustavu putem drugog računalnog sustava te simuliranjem kao da je u pitanju neki sustav s kojim ovlaštena osoba ima vezu povjerenja [22]

[3] U literaturi eng. Scavenging, Dustbin Diving, Dumpster Diving

[4] Metoda poznata pod nazivom eng. Masquerading, Deception

[5] U literaturi se spominje još pod nazivom eng. Exploitation od Trust

2.2.2. Krađa identiteta

Krađom identiteta možemo nazvati svaku radnju u kojoj pojedinac ili skupina ljudi prikuplja tuđe osobne podatke protivno zakonu. Zlouporaba tuđih osobnih podataka na bilo koji način događa se u svrhu nanošenje štete osobi čiji su podatci. Šteta može biti materijalna, može poticati financijske gubitke kod oštećene osobe ili najčešće povredu ugleda i časti kao i povredu privatnosti ujedno je to i kazneno djelo za koje je predviđena i kazna zatvora do godinu dana (za osnovni oblik tog djela). Ukoliko netko protivno uvjetima određenima zakonom iznosi osobne podatke iz Republike Hrvatske u svrhu daljnje obrade ili ih na bilo koji drugi način učini dostupnim drugome ili tko prikupljanjem, obradom podataka ili bilo kojom drugom radnjom sebi ili drugome pribavi imovinsku korist ili prouzroči štetu kaznit će se kaznom zatvora do tri godine. – v. čl. 146. Kazneni zakon (NN:144/12). [9]

Jedan od najčešćih primjera prevare u razvijenom svijetu je pribavljanje koristi putem telekom operatera a uz to i nanošenje štete osobi čiji su podatci. Osoba 1 koristi osobne podatke osobe 2 u svrhu sklapanja "lažnog" ugovora s nekim teleoperaterom, predstavljajući se kao osoba 2, sklopi u njeno ime i na njenu štetu, a u svoju korist ugovor o pribavljanju broja i mobilnog uređaja , napravi račun koji ne podmiruje, a teret dugovanja padne na osobu 2 koja sa spomenutim ugovorom nema nikakve veze budući je isti lažno sklopljen korištenjem njenih osobnih podataka. Tada vrlo često dolazi do ovrha i tužbi od strane odvjetničkog društva. U takvim slučajevima je osobi 2 vrlo teško dokazati da se zaista radi o prevari. U velikim korporacijama postoji problem od krađe osobnih podataka iz kanti za smeće koji se nalaze u uredima. Na primjer, osoba 1 može iskopati iz kontejnera jedne banke čitav niz bačenih izlista sa osobnim podatcima građana koje potom može zloupotrijebiti u svrhu izvršenja kaznenih dijela. Ovakvih primjera ima beskonačno mnogo. Prilikom bacanja bilo kakvih dokumenata s osobnim podatcima u smeće potrebno je dokument uništiti što je više moguće. Poželjno ga je podrapati ili staviti u rezalicu za papir a najsigurniji način bi bilo zapaljenje istog tako da se u rukama krivih ljudi ne može iz njega uzeti osobne podatke. [9]

Potrebno je voditi računa kome se daju osobni podatci. U slučaju da se podatci daju poslodavcu, banci liječniku ili državnim tijelima gotovo sigurno postoji nadzor i kontrola nad obradom tih podataka. Relacije između klijenta i banke, pacijenata i liječnika pa čak građanina i državnog tijela uvijek su pokrivene sigurnosnim protokolima koji osiguravaju zaštitu osobnih podataka a uz to sprječavaju zlouporabu.

U slučaju zlouporabe osobnih podataka ili krađe identiteta potrebno je odmah reagirati i slučaj prijaviti nadležnim službama i policiji uz navođenje svih poznatih činjenica. Ako se radi o lažnim ugovorima, nužno je odmah o tome obavijestiti pravnu osobu s kojom je ugovor sklopljen i po mogućnosti zatražiti snimku s kamere ukoliko je ugovor potpisan na prodajnom mjestu, ukoliko oštećena osoba ne dobije snimku nadzorne kamere onda to mora zatražiti policija, povrh toga se osim što je riječ o kaznenom djelu, radi i o povredi Zakona o zaštiti osobnih podataka, može se podnijeti zahtjev za zaštitu prava Agenciji za zaštitu osobnih podataka. [9] [1]

2.3. Važnost zaštite podataka u virtualnom svijetu

Virtualni svijet odnosno Internet možemo gledati kao najveću svjetsku enciklopediju. Internet se koristi i za komunikaciju, učenje, kupovinu pa čak i zabavu. U virtualnom svijetu osobne podatke dajemo na raznim forumima, društvenim mrežama, raznim on-line igrama, web oglasima, web trgovinama ili raznim drugim stranicama koje zahtijevaju registraciju. Uz sve današnje tehnologije nemoguće je ostati anoniman, svaki poziv, SMS poruka ili komunikacija putem raznih aplikacija ostaju zapisani u virtualnom svijetu. Sve što se objavi na Internetu ne može se trajno obrisati, stoga je potrebno paziti što i gdje objavljujemo. Opasnost u virtualnom svijetu nije uzrokovana samo objavljivanjem osobnih podataka, ona se može pojaviti objavljivanjem slika iz svakodnevnog života gdje bilo tko može vidjeti životne navike pojedinca.

U Zagrebu se moglo čuti za veliku krađu koja se dogodila jednoj osobi iz javnog života za vrijeme boravka u Meksiku. Poznata hrvatska pjevačica je svakodnevno objavljivala veliku broj slika i statusa na svim društvenim mrežama, svi njeni profili su dostupni javno. U trenutku kada se vratila u Zagreb primijetila je da joj je ukraden nakit,

tehnički uređaji i gotovina, a ukupna šteta procjenjuje se na oko 70.000 kuna. Ima veliku broj ovakvih primjera iz kojih se može naučiti da nije dobro sve javno objavljivati.

2.3.1. Tehnika prikupljanja povjerljivih podataka u virtulnom svijetu

XSS (eng. Cross-site scripting) je jedna od najčešće korištenih zlonamjernih tehnika napada u virtualnom svijetu. Unatoč velikom i neprekidnom eksperimentiranju s mnoštvom novih zlonamjernih tehnika još uvijek se najviše koristi XSS.

XSS ranjivost nastaje kada web aplikacije uzmu podatke od korisnika i dinamički ih uključuju u web stranice bez detaljne provjere podataka. Svaki takav napada omogućuje napadaču da u web pregledniku napadnutog korisnika prikazuje svojevoljne komande i uz to prikazuje proizvoljni sadržaj u pregledniku. Na taj način napadač dobiva pristup određenim aplikacijama ili stranicama na način da zaobiđe sigurnosnu provjeru i lozinke napadnutog korisnika. XSS napadom mogu se otuđiti korisnički računi, kompromitirati privatne informacije i slično. Da bi napadač korištenjem web preglednika ispitao odgovor dinamičke stranice, on formulira i distribuira vlastiti XSS URL (eng. Uniform Resource Locator) zahtjev. Napadač također mora poznavati HTML (eng. HyperText Markup Language) i JavaScript jezik da bi proizveo URL koji nije previše sumnjivog izgleda te tako napao stranicu osjetljivu na XSS napade. Kao primjer možemo gledati facebook stranicu koja povremeno korisniku na mail šalje link za verifikaciju mail adrese. Napadač može putem elektroničke pošte poslati poveznicu napadnutom korisniku kako bi isti potvrdio lozinku, otvaranjem poveznice otvara se Internet stranica koja je izgledom vrlo slična ili gotovo ista početnoj stranici facebook-a, napadnuti korisnik u tom trenutku ne može znati da se radi o napadu te upisuje svoje korisničko ime i lozinku. Upisivanjem svojih podataka napadač dobiva podatke kojima može ukrasti račun od facebook profila.

Osim iznad navedenim načinom, napadači se koriste raznim tehnikama kako bi dobili pristup računalnom sustavu. U razvijenim zemljama počinitelji prvotno nastoje pribaviti podatke o računalnom sustavu i načinu na koji se on koristi.

Još jedna od navedenih metoda je eng. Spoofing koji obuhvaća više metoda pomoću kojih napadači dolaze do željenih podataka, a sve se temelji na slabostima Internet protokola i nedovoljnom pažnjom korisnika.

- Prva od pod metoda Spoofinga je Login Spoofing. Navedena metoda je metoda lažnog predstavljanja putem sličnih maski za upis korisničkih lozinki prilikom pristupanju nekom računalnom sustavu. Pri samom napadu korisnik ne zna da nije pristupio željenom sustavu niti zna da su njegovi podatci dostupni napadaču.
- Druga pod metoda naziva se eng. Web Spoofing i temelji se na nepažnji korisnika koji zabunom odabire pogrešan hiperlink[6] i dolazi na neželjenu stranicu a da nije ni svjestan da se nalazi na krivoj stranici, (npr. www.isuv.hr umjesto www.isvu.hr)
- Treća pod metoda naziva se eng. E-mail Spoofing, to je ujedno metoda u kojoj se hakeri koriste slabostima SMTP[7] protokola za slanje elektroničke pošte; promjenom podataka od koga je pošta poslana kako bi dobili odgovor od primatelja.
- Kao četvrta pod metoda spominje se eng. DNS Spoofing u kojoj se hakeri koriste načinom na koji se na Internetu traže brojčane adrese računala pomoću njihovog simboličkog ekvivalenta. DNS[8] tada omogućava traženje brojčanih Internet adresa putem simboličkog ekvivalenta preko DNS servera na kojem se nalazi datoteka s traženim podatcima. Napadač ima cilj presresti komunikaciju između ovlaštenog računalnog sustava i DNS servera kako bi mogao poslati lažne podatke u računalni sustav koji želi napasti. Ukoliko napadač uspije

[6] Eng.Link ili poveznica, klikom miša na poveznicu otvara se neka Internet stranica

[7] SMTP, od engl. Simple Mail Transfer Protocol, uobičajeni je način (standard) za prijenos elektroničke pošte na internetu

[8] Eng. Domain Name Service

izvršiti napad, sva komunikacija ide preko njegovog računala i on je u mogućnosti prikupiti sve potrebne podatke.

- IP Spoofing kao peta pod metoda koristi se kako bi napadačima omogućio neovlašteni pristup računalima ili računalnim mrežama na daljinu. Napad se vrši izvana, na daljinu kao da je u pitanju ovlašteno računalo iz neke mreže kojoj napadač želi pristupiti. Radi se presretanju i zamjeni IP adresa u zaglavlju paketa koji se prenose. Stariji modeli usmjerivača[9] nisu sposobni prepoznati jeli riječ o podatcima koji se prenose unutar lokalne mreže ili dolaze izvana.
- Šesta pod metoda Probe ili Guessing [10] je pokušaj da se pristupi sustavu nasumičnim pogađanjem lozinke koristeći metodu pokušaja i pogreške.
- Sedma pod metoda naziva se metoda Pretraživanja [11] sastoji se od većeg broja neovlaštenih pokušaja kako bi se pristupilo sustavu ili kako bi se došlo do informacija o samom sustavu uz pomoć nekog automatiziranog alata. Ovakav program je vrlo lako nabaviti putem interneta pa ga najčešće koriste napadači početnici, koji nemaju puno iskustva s drugim pod metodama. Neki od poznatijih aplikacija za ovu vrstu napada nazivaju se eng. War Dialing ili eng. Demon Dialing, neki čak i samu pod metodu Pretraživanja poznaju pod nazivima aplikacija koje se koriste pri napadu.
- Prisluškivanje (eng. Wiretapping) smatra se da se ovom pod metodom prisluškuju telefonske linije za prijenos podataka radi pribavljanja lozinki ili ugrađuju prislušni uređaji na telefonske linije unutar samog računalnog centra.

[9] Usmjerivač se u literaturi još naziva eng. router a to je uređaj koji usmjerava prijenos podataka od jedne računalne mreže ka drugoj, vodeći računa da se to izvede na što efikasniji način

[10] Naziv pod metode u Hrvatskoj literaturi se još naziva Ispitivanje ili pogađanje

[11] Eng. naziv u stranoj literaturi je Scanning

- Optičko špijuniranje (Optical Spying) je promatranje ili snimanje iz obližnje zgrade. Presretanje elektromagnetskog zračenja s ekrana računala kako bi se postigla optička špijunaža.
- Pod metoda „Druženje“ (eng. Socializing) je neformalno druženje sa zaposlenicima poslije radnog vremena kako bi se od njih dobile informacije o samom sustavu, mjerama zaštite i drugim okolnostima koje se mogu iskoristit za pristup sustavu.

2.3.2. Privatnost i zaštita osobnih podataka na internetu

Društvene mreže potiču sve veće zadiranje u privatnost pojedinca. Povećanjem broja korisnika društvenih mreža ali i drugih web portala povećava se i količina podijeljenih informacija koje korisnici objavljuju. Vrlo rasprostranjena društvena mreža kao što je Facebook dosta pozornosti pridaje zaštiti osobnih podataka. Postavke korisničkog računa su toliko kompleksne i imaju toliko mogućnosti da bi se većina ljudi trebala dobro pozabaviti kako bi zaštitili svoje podatke. Sigurnost takvih mreža je postala vrlo kompleksan problem jer razne postavke na Facebooku i sličnim mrežama zahtijevaju više pozornosti i vremena nego što su sami korisnici spremni izdvojiti.

Skrivanje podataka o korisnicima nije u interesu većih društvenih mreža jer one te podatke koriste za oglašavanje, slanje ponuda velikim i malim poduzetnicima i tvrtkama. Na kraju, glavni razlog što uopće možete koristiti stranice poput Facebooka besplatno je upravo taj što oni oglašivačima prodaju pristup vama te vašim interesima i navikama. Najčešće Internet stranice znaju o svojim posjetiteljima nego što oni to misle. Kao dobar primjer može poslužiti bilo koji internetski portal na kojem čitatelji mogu pogledati najnovije vijesti. Svaka stranica ili svaki portal koji ima prostor za oglašavanje dijeli se na *eng. Leaderboard*, desni stupac, lijevi stupac, naslovnica sredina lijevo, naslovnica sredina desno, *eng. Floating*, te naslovnica iznad boxa izbora urednik.

Pri pregledavaju Internet stranica web preglednik može prikazivati oglase na temelju različitih čimbenika:

- Vrste web stranice koju posjećuje korisnik i aplikacije koje ima na mobilnom uređaju
- Kolačići na pregledniku i postavke na Google računu korisnika
- Web stranice i aplikacije koje je korisnik posjetio a da pripadaju tvrtkama koje oglašavaju s Googleom
- Aktivnost korisnika na drugom uređaju
- Prethodne interakcije s Googleovim oglasima ii uslugama oglašavanja

- Aktivnosti i informacije s Goolgeovim oglasima ili uslugama oglašavanja

Prilikom prikazivanja prilagođenih oglasa Google nikada neće povezivati identifikatore s kolačića ili sličnih tehnologija s osjetljivim kategorijama kao što su oglasi koji se temelje na rasi, vjeri, seksualnoj orijentaciji ili zdravlju. [12][13]

Kao dobar primjer može se uzeti slučaj gdje korisnik traži smještaj preko Booking-a za lokaciju na kojoj nikada nije bio, za primjer se može uzeti grad Malaga u Španjolskoj. To mjesto stanovništvu Republike Hrvatske nije toliko česta točka interesa kao neki drugi gradovi u Europi da bi sustav mogao svojevoljno oglašavati smještaj za gradove poput Londona, Pariza i slično. Google pretraživač je pokupio kolačiće koji skupljaju Vaše podatke i putem njih dobiju informaciju da Vas zanima smještaj u Malagi i na osnovu prikupljenih informacija idućih nekoliko dana će korisniku oglašavati ponude smještaja u Malagi i okolnim mjestima. Iz navedenog primjera može se zaključiti da i ako ne dajete nikakve podatke na Internet i nigdje se ne registrirate i dalje nemate stopostotnu privatnost.

Najčešći od praktičnih razloga koji se potežu o raspravama o privatnosti i zaštiti podataka su oni vezani za osobni ugled. Kako profili na Facebooku i ostalim društvenim mrežama itekako mogu utjecati na sveopći dojam koji ljudi mogu steći o osobi koju „proguglaju“ i to je nešto što svakako treba imati na umu pri dijeljenju raznih informacija na takvim stranicama. Svijest o vlastitom ugledu na webu većina ljudi već uglavnom ima kada se govori o općenitim društvenim situacijama poput stvaranja novih poznanstava, ali postoji i znatan broj situacija u kojima je teže predvidjeti da će upravo vaš Facebook profil odigrati ključnu ulogu te kakva će ta uloga biti, pozitivna ili negativna. Nakon slanja životopisa u neku firmu, poslodavac je osoba koja će prije razgovora za posao posegnuti za profilom osobe koja je poslala životopis kako bi saznao što više informacija. Oni to najčešće čine kako bi provjerili podatke iz životopisa i molbe, ali i da bi se uvjerili kako kandidati nemaju nekih većih osobnih problema koji bi mogli utjecati na njihov rad. Alkoholizam i konzumacija težih droga spadaju u tu kategoriju. Razne predrasude vezane za dob, spolnu orijentaciju, političku i vjersku opredijeljenost ili invaliditet također mogu zakomplicirati stvari, jer iako na njih zakon ne gleda blagonaklono, izuzetno ih je teško dokazati na sudu. Istu provjeru

može napraviti i osoba od koje korisnik želi unajmiti stan. Takvom provjerom vlasnik stana dobio bi informacije dali osoba ima naviku raditi tulume, uništavati imovinu i raditi bilo kakve druge neželjene stvari. [10][11]

Zaštiti se na Internetu je moguće ukoliko se pazi što se sve objavljuje i kakve se slike dijele s prijateljima s društvene mreže. Putem Facebooka ili bilo koje druge mreže nije potrebno ej dobro promisliti prije dijeljenja bitnih podataka koji mogu donijeti nezgodne posljedice ukoliko dođu u posjed krivih osoba. Čak i uz najbolje namjere, uvijek postoji mogućnost da neka greška *(eng.bug)* u samom softwareu omogući krivim ljudima pristup vašim privatnim porukama, kao što se dogodilo u svibnju 2010. godine, kada je greška u Facebookovom sistemu dozvolila korisnicima da čitaju poruke svih svojih kontakata. Iako se takvi propusti u sigurnosti uvijek vrlo brzo isprave, potencijal za štetu koju curenje takvih informacija može uzrokovati je ogroman. [10][11]

Najbitnije pravilo vezano za sigurnost na društvenim mrežama je nikada ne smetnuti s uma da sve što stavite na njih može u nekom trenutku postati javno te zauvijek dostupno svakom tko traži takvu vrstu informacija o vama.[10][11]

2.3.3. Prikupljanje podataka i identifikacija

Zbog potrebe pristupanja nekom računalnom sustavu fizičkim pristupom ili daljanskim pristupom u praksi brojnih zemalja pojavljuju se različiti identifikacijski sustavi. U virtualnom svijetu svaki čovjek ostavlja trag.[12] Eng Cookies se pohranjuju u preglednicima i računalima, a poznati su kao tekstualne informacije pohranjene u formi diska na našem računalu. Kolačići omogućavaju automatsko spajanje na web

[12] Elektronički trag je trag koji čovjek ostavlja iza sebe a može biti u obliku povijesti preglednika, kolačića i slično

poslužitelj, prikazuju nam ono što želimo vidjeti.[13] Kolačići omogućavaju automatsko spajanje na web poslužitelj, prikazuju nam ono što želimo vidjeti, to su najčešće informacije koje se mogu gledati bez dodatne naplate. Sve informacije o našim interesima, kretanju, zanimanjima, našim navikama i slično neke osobe mogu prikupiti i zlorabiti s ciljem dolaženja do novih spoznaja i nanošenja socijalne ili financijske štete. Velika količina osobnih podataka završi na internetu jer ih korisnici sami daju na način da ispunjavaju razne formulare za registraciju. Prikupljanje, povezivanje i analiziranje takvih podataka stvara sliku i profil velikog broja korisnika interneta. Kao dobar primjer zarade na osobnim podatcima je Konzumova Multiplus kartica koju pri svakoj kupnji kupci provuku kroz blagajnu. Prilikom registracije Multiplus kartice svaki kupac dužan je ostaviti svoje podatke kao što su ime, prezime, adresa, e mail adresa, broj ukućana i slično. Provlačenjem kartice i skupljanjem bodova program (eng.software)[14] evidentira što se sve nalazi na računu i na taj način stvara profil kupca. Prema tome osoba koja ima pristup podatcima koji se prikupljaju u nekoj bazi podataka može točno znati koja osoba kupuje koje stvari, što ta osoba voli jesti, prikupljanjem podataka o prodajnom mjestu može se dobiti informacija gdje se osoba najčešće kreće. Čak je moguće na taj način dobiti informaciju dali je osoba samac ili ima obitelj i malu djecu, takav podatak je najlakše otkriti ako se u bazi podataka izdvoje kupci koji kupuju dječje kašice ili pelene. Takvih primjera ima bezbroj, a analizom i obradom prikupljenih podataka poslovnice Konzuma svakom kupcu izdaju bon s popustom za kupovinu određenog artikla. Prema nekim procjenama tržište osobnih informacija, već je 1999. godine premašilo vrijednost od 1,5 milijardi dolara. U današnje vrijeme gdje se sve više podataka prikuplja putem socijalnih mreža nemoguće je utvrditi točnu vrijednost takvog tržišta. Sve je veća količina osobnih

[13] Preglednik prati stranice koje gledamo i prema tome određuje naše točke interesa kako bi na prostoru za oglašavanje sa korisnik ponudio ono što ga zanima.

[14] Računalni Software je računalni program napisan tako da je njegov sadržaj lagano promijeniti. Stručno značenje pojma softvera je da su to računalni programi pisani (registrirani) u hardverske komponente u digitalnom obliku a dostupan je mikroprocesoru računala (tvrdi disk, USB disk, kompaktni diskova, itd).

podataka koji se o korisnicima interneta prikupljaju na brojnim web-stranicama, što nije popraćeno dovoljno jakim mjerama zaštite. Prikupljenim podatcima se koriste i potencijalni poslodavci odlučujući o nečijem zaposlenju ili čak i kriminalci radi raznih iznuda.[16][19]

3. Postojeća (dosadašnja) pravna regulativa

Zakon o zaštiti osobnih podataka donesen je zbog zaštite osobnih podataka odnosno zaštite privatnog života pojedinca. Dakle, zaštita osobnih podataka je ustavna kategorija. U Republici Hrvatskoj osigurana je zaštita osobnih podataka svakoj fizičkoj osobi bez obzira na državljanstvo i prebivalište, rasno ili etničko podrijetlo, politička, vjerska ili druga opredjeljenja.

3.1. Vijeće Europe – Konvencija 108 za zaštitu osoba glede automatizirane obrade osobnih podataka (Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data)

Konvencija 108 donesena je 28. siječnja 1981. godine a potpisana je i od strane Republike Hrvatske, 5. lipnja 2003. u Strasbourgu. Svrha Konvencije je svakoj fizičkoj osobi, osigurati poštovanje njezinih prava i temeljnih sloboda a osobito na privatnost glede automatizirane obrade podataka koji se odnose na zaštitu podataka, bez obzira na njezino državljanstvo i boravište.

Konvenciju su potpisale sve države članice Vijeća Europe u cilju ostvarivanja jedinstva između svojih članica posebno na vladavini prava, ljudskih sloboda i temeljnih sloboda, ostvarivanje prava na privatnost glede automatizirane obrade osobnih podataka koji se na nju odnose.

Hrvatski Sabor je 14. travnja 2005. godine donio Zakon kojim potvrđuje Konvenciju za zaštitu osoba glede automatizirane obrade osobnih podataka i Dodatnog protokola uz konvenciju za zaštitu osoba glede automatizirane obrade osobnih podataka u vezi nadzornih tijela i međunarodne razmjene podataka.

Prema članku 4. dužnost svake stranke je poduzimati potrebne mjere kako bi ostvarila temeljna načela za zaštitu osobnih podataka. Svaka stranka potrebne mjere mora poduzeti najkasnije u trenutku stupanja Konvencije na snagu za tu stranku.

Člankom 5. konvencije su definirana svojstva podataka gdje svi osobni podatci koji su predmet automatizirane obrade podataka trebaju biti pribavljeni i obrađeni u dobroj vjeri i zakonito, uz to moraju biti pohranjeni u određene i zakonite svrhe te ne smiju biti upotrjebljene na niti jedan drugi način. Svi osobni podatci moraju biti točni i ažurirani, sačuvani u obliku koji omogućuje identifikaciju subjekata podataka tijekom razdoblja koje nije duže nego što nalaže svrha u koju su pohranjeni. Člankom je određeno da podatci moraju biti odgovarajući mjerodavni i ne suvišni u odnosu na svrhe u koje su pohranjeni, uz to ih je potrebno ažurirati po potrebi kako bi uvijek bili točni i sačuvani u obliku koji omogućuje identifikaciju subjekata podataka tijekom razdoblja koje nije duže nego što nalaže svrha u koju su pohranjeni.

3.2. Direktiva 95/46/EZ Europskog parlamenta i Vijeća - Direktiva o zaštiti pojedinca u vezi s obradom osobnih podataka i o slobodnom protoku takvih podataka

Europski parlament i Vijeće su 24. kolovoza 1995. godine donjeli Direktivu 95/46/EZ kojoj je cilj bio zaštiti pojedince po pitanju obrade osobnih podataka i slobodnom protoku takvih podataka. Jasno je definiran problem koji se pojavio kada su u pitanju osobni podatci te sama zaštita istih. Direktiva se donijela radi poboljšanja odnosa u zajednici više naroda te budućih ciljeva zajednice. Nove izmjene i dopune su napravljene kako bi se poboljšao ekonomski i društveni napredak koji je u to vrijeme dijelio Europu. Temelj Direktive je poticanje boljih odnosa u regiji te jačanje mira i slobode uz promicanje demokracije priznate po ustavu i zakonima država članica uz pridavanje pažnje zaštiti ljudskih prava i temeljnih sloboda. Jedna od stavki ugovora spominje i sustave za obradu podataka koji prema riječima iz ugovora su dizajnirani da služe čovjeku bez obzira na nacionalnost ili boravište, s ciljem doprinosa na društvenom i ekonomskom napretku, te poticanje napretka trgovina i pojedinca.

Ugovorom je predviđeno da ciljevi zajednice obuhvaćaju stvaranje čvršćeg saveza između europskih naroda, učvrstujući odnose među državama u Zajednici, potičući i osiguravajući gospodarski i socijalni napredak uz uklanjanje zapreka koje

razdvajaju Europu. Veliki naglasak je stavljen na poboljšanje uvijeta života svih naroda uz jačanje mira i slobode te promicanje demokracije n temelju temeljnih prava koja su priznata po ustavu i zakonima zemalja članica.[5]

Članak 11. se odnosi na prikupljanje osobnih podataka kada oni nisu dobiveni od osobe čiji se podatci obrađuju. Podatci se moraju koristiti u poštene svrhe, stim da se osobi čiji se podatci obrađuju moraju dostaviti podatci nadzornika ili zamjenika. Države članice propisuju da nadzornik ili zamjenik moraju u trenutku bilježenja osobnih podataka ako je predviđeno otkrivanje trećoj stranci ili najkasnije u trenutku kada su podatci prvi puta otkriveni, dati osobi čiji se podatci obrađuju barem podatke o identitetu nadzornika i njegovog zastupnika, navesti svrhu obrade podataka ili bilo koji daljnji podatak o primateljima, vrstama primatelja podataka, postojanju prava na pristup podatcima i pravo na ispravljanje podataka. Prikupljač osobnih podataka mora dati jamstvo poštene obrade u osnosu na osobu čiji se podatci obrađuju.

Gore navedeno ne primjenjuje se, za obradu u statističke svrhe ili svrhe povjesnog ili znanstvenog istraživanja, kada je davanje takvih podataka nemoguće ili ako je bilježenje ili otkrivanje iričito propisano zakonom. U slučaju takvih prikupljanja podataka sve države članice propisuju odgovarajući zaštitu. [5]

Članak 16. navodi da svaka osoba koja djeluje po ovlaštenju nadzornika ili obrađivača, uključujući i samog obrađivača, koja ima pristup osobnim podacima ne smije ih obrađivati osim na temelju uputa nadzornika i ako mu zakon tako nalaže. [5]

3.3. DIREKTIVA 2002/58/EZ EUROPSKOG PARLAMENTA I VIJEĆA - o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija (Direktiva o privatnosti i elektroničkim komunikacijama)

Direktiva je donesena 12. srpnja 2002. godine u Bruxellesu s ciljem pojašnjavanja i nadopunjavanja Direktive 95/46/EZ uz usklađenja odredbe država članica koje trebaju osigurati ujednačenu razinu temeljnih prava i sloboda. Najveći cilj je osigurati pravo na privatnost osobnih podataka na području elektroničkih komunikacija i kretanju istih.

Ovom direktivom obuhvaćena su pravila po pitanju pružanja usluga elektroničkih komunikacija i pretplatničkih linija spojenih na digitalnu centralu. Direktiva stupa na snagu s danom objavljivanja u Službenome listu Europskih zajednica.

Člankom 2. određeno je da se definicije iz Direktive 95/46/EZ i Direktive 2002/21/EZ i dalje primjenjuju osim ako nije drugačije određeno:

"(a) «korisnik» označava svaku fizičku osobu koja koristi javno dostupnu elektroničku komunikacijsku uslugu, u privatne ili poslovne svrhe, pri čemu nije nužno da se pretplatila na tu uslugu;

(b) «podaci o prometu» označavaju bilo koje podatke koji se obrađuju u svrhu prijenosa komunikacije na elektroničkoj komunikacijskoj mreži ili za njezino naplaćivanje;

(c) «podaci o lokaciji» označavaju bilo koje podatke obrađene u elektroničkoj komunikacijskoj mreži, koji naznačuju zemljopisni položaj terminalne opreme korisnika javno dostupne elektroničke komunikacijske usluge;

(d) «komunikacija» označava svaku informaciju koja se razmjenjuje ili prenosi između ograničenog broja strana putem javno dostupne elektroničke komunikacijske usluge. Ovo ne uključuje bilo koju informaciju prenesenu kao dio usluge emitiranja za javnost putem elektroničke komunikacijske mreže, osim u onoj mjeri u kojoj se informacija može odnositi na pretplatnika ili na korisnika koji prima informaciju koji se mogu identificirati;

(e) «poziv» označava vezu uspostavljenu putem javno dostupne telefonske usluge koja omogućuje dvosmjernu komunikaciju u stvarnome vremenu;

(f) «pristanak» korisnika ili pretplatnika odgovara podacima o pristanku osobe iz Direktive 95/46/EZ;

(g) «usluga s dodatnom vrijednosti» označava svaku uslugu koja zahtijeva obradu podataka o prometu ili lokaciji osim podataka o prometu koji nisu nužno potrebni za prijenos komunikacije ili za njeno naplaćivanje;

(h) «elektronska pošta» označava svaku tekstualnu, glasovnu, zvučnu ili slikovnu poruku poslanu preko javne komunikacijske mreže koja se može pohraniti u mreži ili u primateljevoj terminalnoj opremi sve dok ju primatelj ne preuzme.“ [5] [6]

Člankom 4. govori da pružatelj javno dostupnih komunikacijskih usluga mora poduzeti sve potrebne mjere kako bi zaštitio sigurnost svojih usluga. U slučaju bilo kakvih napada ili opasnosti pružatelj javno dostupne komunikacijske usluge dužan je obavijestiti pretplatnike o opasnosti. S obzirom na sva najnovija dostignuća i trošak njihove provedbe, navedene mjere moraju osigurati razinu sigurnosti koja odgovara prikazanim opasnostima. Pružatelj javno dostupne elektroničke komunikacijske

usluge dužan je obavijestiti pretplatnike o bilo kakvoj opasnosti ili narušavanju sigurnosti mreže. Ako se pojavi opasnost izvan opsega mjera koje treba poduzeti pružatelj usluge on je i dalje dužan svim sredstvima otkloniti opasnost uključujući i naznaku vjerojatnih troškova koji bi se mogli pojaviti u svezi toga. [6]

Direktivom je doneseno pravilo gdje pružatelj usluga mora svakom pretplatniku omogućiti pravo zabrane prikaza broja pozivatelja a isto tako je pružatelj usluga dužan svakom pozvanom pretplatniku omogućiti sprječavanje prikaza broja pozivatelja kod dolaznih poziva bez naplate.[6]

Direktiva 95/46/EZ i Direktiva 2002/21/EZ u članku 9. donosi pravilo na prijenos podataka o lokaciji koji nisu podatci o prometu. Naime, svi podatci o korisnicima koji se prikupljaju smiju ići u obradu tek nakon što ih se učini anonimnima odnosno uz pristanak korisnika ili pretplatnika. Pružatelj usluga mora obavijestiti korisnike ili pretplatnike o vrsti podataka o lokaciji koji nisu podatci o prometu koji će se obraditi, o svrsi i trajanju obrade te hoće li se ti podatci proslijediti trećoj osobi u svrhu pružanja usluga dodatne vrijednosti. Stavka 2. navedenog članka kaže da i nakon dobivanja pristanka korisnika ili pretplatnika na obradu podataka on i dalje ima pravo na jednostavan način i bez naplate privremeno odbiti obradu takvih podataka.

Obrada svih ostalih podataka koji nisu podatci o prometu u skladu sa stavcima mora se ograničiti na osobe koje djeluju pod nadzorom pružatelja telekomunikacijske usluge. Svi podatci koji nisu podatci o prometu, a odnose se na korisnike javnih telekomunikacijskih operatera, mogu se obraditi samo nakon što se ti podatci učine anonimni, uz pristanak korisnika, u mjeri i u trajanju potrebnome za pružanje usluge s dodatnom vrijednošću. Pružatelj usluga je dužan obavijestiti korisnike o vrsti podataka o lokaciji koji nisu podatci o prometu, o svrsi i trajanju obrade. Pružatelj usluga mora korisnika upozoriti ukoliko će se dotični podatci proslijediti trećoj osobi u svrhu pružanja usluge s dodatnom vrijednosti. Korisnicima ili pretplatnicima treba se pružiti mogućnost opoziva njihova pristanka na obradu podataka o lokaciji koji nisu podaci o

prometu u bilo koje vrijeme bez davanja bilo kakvih razloga zbog kojih korisnik želi opozvati pristanak na obradu podataka.

Svaki korisnik nakon davanja svog pristanka na obradu podataka ima pravo i mora imati mogućnost na jednostavan način i bez ikakve naplate privremeno odbiti obradu takvih podataka za svako priključivanje na mrežu ili za svaki prijenos komunikacijskih usluga. Obrada podataka o prometu mora se ograničiti na osobe koje djeluju pod nadzorom pružatelja javne komunikacijske mreže, odnosno treće osobe koja pruža uslugu s dodatnom vrijednosti, te mora ograničiti na ono što je nužno u svrhu pružanja usluge s dodatnom vrijednosti. [6]

Kao još jedna mjera zaštite podataka korisnika je obavještavanje korisnika, kojim države članice osiguravaju da pretplatnici budu obaviješteni ukoliko je njihov broj dostupan u javnom telefonskom imeniku. Članak 12. stavka 2. kaže da sve države članice osiguravaju pretplatnicima mogućnost kojom oni mogu odrediti hoće li njihovi osobni podatci biti uključeni u javni telefonski imenik ili ne. Ukoliko hoće korisnik ima pravo odlučiti koji podatci i u kojoj mjeri su ti podatci relevantni za svrhu telefonskog imenika koju je odredio pružatelj, isto tako pretplatnik ima mogućnost provjeriti, ispraviti ili opozvati takve podatke iz imenika bez dodatne naplate. [6]

3.4. Agencija za zaštitu osobnih podataka

Glavna regulatorna agencija za zaštitu pojedinaca i njihovih podataka u Hrvatskoj je Agencija za zaštitu osobnih podataka (AZOP). Jedna od zadaća i obaveza agencije je sudjelovanje u radnim skupinama i raznim međunarodnim konferencijama. Republika Hrvatska kao članica Vijeća Europe aktivnim radom AZOP-a na međunarodnoj sceni pridonosi razvoju, poboljšanju zakona, usklađivanju zakonodavstva Republike Hrvatske u području zaštite osobnih podataka pojedinaca s svjetskim normama i standardima. Sve članice EU-a dužne su prema Direktivi ZOP uspostaviti tijela koja obavljaju nadzor nad pravilnom primjenom propisa o zaštiti osobnih podataka s potpunom neovisnošću. Osnivanje neovisnih tijela smatra se ključnim sastavnim dijelom zaštite pojedinca u vezi s obradom osobnih podataka. U pravu EU se uvjet neovisnosti nadzornih tijela za zaštitu osobnih podataka izričito

utvrđuje i Ugovorom o funkcioniranju Europske unije te Poveljom o temeljnim pravima EU-a. [20]

Misija Agencije za zaštitu podataka je izvršavanje nadzora nad provođenjem propisa o zaštiti osobnih podataka, ukazivanje na zlouporabe koje se događaju pri prikupljanju osobnih podataka, te rješavanje zahtjeva za utvrđivanje povrede zajamčenih prava Zakonom o zaštiti osobnih podataka svakom pojedincu u Republici Hrvatskoj. [7] [1][20]

Agencija za zaštitu podataka nastoji davati preporuke za unaprjeđenje zaštite osobnih podataka kod voditelja obrade, davati savjete u svezi s uspostavom novih zbirki osobnih podataka, naročito u slučaju uvođenja nove informacijske tehnologije. Misija Agencije za zaštitu osobnih podataka također je i praćenje uređenja zaštite osobnih podataka u drugim zemljama. I suradnja s nadležnim tijelima za nadzor osobnih podataka u njima.

Vizija Agencije je uspostavljanje i očuvanje visoke razine zaštite osobnih podataka kao jednog od temeljnih ljudskih prava. Novi zakonodavni instrumenti Europske unije doneseni su 2016. godine a početak će se primjenjivati od svibnja 2018. godine. Prema mišljenju Agencije potrebno je stalno osvješćivati građane o potrebi i važnosti zaštite privatnosti i zaštite osobnih podataka kao glavnog i temeljnog ljudskog prava, posebno u današnje vrijeme s obzirom na stalni razvoj tehničkih dostignuća i mrežnog povezivanja ljudi koji uzrokuju kolanje velikih količina podataka. S obzirom na stalni razvoj tehničkih mogućnosti obrade osobnih podataka potrebno je stalno pratiti dostignuća primjenjiva u Hrvatskoj kako bi se pravnom praksom Agencije regulirala obrada osobnih podataka. Posao Agencije je osigurati redovitu razmjenu iskustava s drugim tijelima javne vlasti u Hrvatskoj a tako i s međunarodnim tijelima za zaštitu osobnih podataka, najčešće s državama članicama Europske unije.[7]

Prilikom obavljanja poslova nadzora Agencija ima sve ovlasti za izdavanje upozorenja i opomena voditeljima zbirki, primateljima osobnih podataka te izvršiteljima obrade ukoliko uoči neke nezakonitosti. U slučaju nezakonitosti agencija ima pravo narediti da se nepravilnosti uklone i da se obrada podataka obustavi, a čak ima pravo i narediti brisanje podataka ako su prikupljeni bez pravne osnove. Agencija rješenjem

može zabraniti nezakonito iznošenje podataka iz Republike Hrvatske ili njihovo nezakonito davanje na korištenje primateljima, ili pak zabraniti povjeravanje poslova njihove obrade izvršiteljima obrade koji ne ispunjavaju tražene uvijete u pogledu zaštite osobnih podataka. Žalbe protiv Agencije nisu dopuštene, ali se može tražiti pokretanje upravnog spora. [15]

Tablica 1. Strateški plan AZPS 2017-2019 [7] [14]

STRATEŠKI PLAN AZPŠ 2017-2019				
Opći cilj	Posebni cilj	Pokazatelj učinka	Način ostvarenja	Pokazatelj rezultata
1	2	3	4	5
Podizanje razine zaštite osobnih podataka	Osiguravanje učinkovite provedbe zakona I propisa o zaštiti osobnih podataka	Smanjen broj uočenih zlouporaba	Nadzor provedbe zaštite osobnih podataka	Kontinuirana realizacija planiranih nadzora I nadzora po zahtjevu za zaštitu prava
			Podizanje razine svijesti građana I popularizacija područja zaštite osobnih podataka	Kontinuirano održavanje različitih oblika osvješćivanja javnosti I edukacija za voditelje obrade, službenike za zaštitu osobnih podataka i građane
			Rješavanje povodom zahtjeva za utvrđivanje povrede prava zajamčenih Zakonom o zaštiti osobnih podataka	Kontinuirano rješavanje neupravnih predmeta u zakonskim rokovima
				Kontinuirano praćenje predmeta I njihovo rješavanje u I. stupanjskom upravnom postupku u zakonskim rokovima
			Provođenje nadzora prema Uredbi o Hrvatskom viznom informacijskom sustavu	Kontinuirana realizacija planiranih nadzora diplomatskih misija I konzularnih ureda RH u svijetu na godišnjoj razini

			Donošenje zakonskih I pod zakonskih akata odnosnih na područje zaštite osobnih podataka	Izmjene I dopune zakonskih I pod zakonskih akata objavljene u Narodnim novinama I stupite na snagu

4. Razlozi potrebe donošenja novih propisa

Vodeće mjesto u razvoju čovjeka ima interes za druženje i komunikaciju na daljinu. Čovjekova inteligencija razvija se kroz druženje i komunikaciju sa drugim ljudima a uz to dolazi do izražaja i čovjekova inteligencija. Nakon informacijske revolucije [15] dolazi do prestanka komunikacije putem mimike i slikovnog izražavanja i počinje moderno sporazumijevanje među ljudima i razmjena informacija. Nakon informatičke revolucije[16] ljudi počinju koristit današnje metode komunikacije na daljinu.

4.1. Tehnološki razlozi donošenja novih propisa

Davne 1440. godine započela je prva informacijska revolucija potaknuta pronalaskom prvog tiskarkog stroja[17], izumio ga je Johannes Gutenberg[18]. Druga informacijska revolucija započinje 1840. godine izumom telegrafa (Morse), a 35 godina kasnije izumljen je prvi telefon koji je omogućio komunikaciju na daljinu. Sredinom dvadesetog stoljeća počinje treća informacijska revolucija te se pojavljuju prva računala. Elektromehanička obrada podataka napravila je veliki pomak a još veći i brži pomak uzrokovala je elektronička tehnologija digitalnom obradom podataka. Teorijske osnove za rad suvremenih računala razvio je 1833. godine C.Babbage. 1944. godine H. Aicken konstruira prvo računalo pod nazivom Mark 1 velikih razmjera

[15] Sredinom 15. stoljeća dolazi do raznih tehničkih otkrića i odgovarajućih tehnoloških postupaka što je dovelo di povijesnog zaokreta u komunikaciji

[16] Informatička revolucija se odnosi na tehnička rješenja koja su omogućena uz pomoć modernih informatičkih i komunikacijskih postrojenja, strojeva, uređaja i mreža koji omogućuju obradu i pohranu podataka, prijenos slika, glasa i zvuka u digitalnom obliku.

[17] Gutenberg je 1440. godine konstruirao je drvenu prešu pomoću koje se dobivao otisak pritiskom ravne ploče, ispunjene metalnim slovima, preko lista papira.

[18] Johannes Gutenberg je njemački tiskar, izumitelj tipografije u Europi, pravim imenom Johannes Gensfleisch zum Gutenberg

s mnoštvom releja koji imaju problema s pregrijavanjem. ENIAC[19] je prvo elektroničko računalo koje je služilo za znanstvene svrhe od 1946. do 1955. godine, konstruirano od strane Eckert, Mauchly i von Neumann-a. [21][22]

Proizvodnja računala za komercijalnu obradu podataka počinje s UNIVAC-om.[20]

Računala možemo podijeliti na šest generacija.

- Prva generacija u uporabi je od 1951.do 1958. godine a koristi elektronske cijevi i kabelske veze pri obradi podataka
- Druga generacija se pojavljuje 1959. i traje do 1963. godine a upotrebom tranzistora i tiskanih krugova s magnetskim jezgrama postiže više
- Treća generacija se koristi od 1964. do 1970. godine uvodi i razvija tehnologiju integriranih krugova i počinje s korištenjem viših programskih jezika
- Četvrta generacija traje od 1971. do 1987. godine i u tom periodu postiže najviše do sada integriranjem poluvodičkih sklopova
- Peta generacija pojavljuje se 1989. godine i ostaje u uporabi do 1992. godine te razvija kompjutore na osnovi paralelne arhitekture i arsenid čipova[21]
- Šesta generacija (od 1993.) usavršavaju se neuroračunala[22] na osnovi neuronske mreže, primjene umjetne inteligencije i iskorištavanja ekspertnih sustava u ostvarivanju postavljenih ciljeva. [23] [24]

---

[19] Electronic Numerical Integrator and Calculator

[20] Universal Automatic Computor

[21] Gallij arsenid (GaAs) je spoj elementa galija i arsena. To je III-V izravni pojasni poluvodički poluvodič s kristalnom strukturom cinka

[22] Neuroračunala su računala koja bi se temeljila na načelima računanja i učenja mehanizama koji su pronađeni u mozgu, a istovremeno bi imali sposobnost steći nova znanja , poznatiji kao umjetna inteligencija

4.2. Usporedba brzine obrade podataka nekada i danas

Jedan od vrlo bitnih razloga uvođenja novih standardan i zakona je promjena u brzini brade podataka. Da bi se 1950-ih obradila neka manja količina podataka koristio se ENIAC koji je zauzimao cijelu halu a težio je 30 tona. Sastojao se od 17,468 vakumskih cijevi, 70,000 otpornika, 1,500 releja i 6,000 ručnih prekidača a uz to sve zauzimao je 167 metara kvadratnih uz potrošnju od 160 kW. Cijena takvih uređaja zbog same mase i dimenzija je bila vrlo visoka i nedostižna prosječnom čovjeku. Zbog takvih razloga vrlo mali broj ljudi se koristio obradom podataka u svrhu napada i bilo im je vrlo lako ući u trag. U današnje vrijeme procesor koji obrađuje puno veću količinu podataka od prvih računala, teži par grama a cijelo super računalo nekoliko kilograma, te uz to ima pristupačnu cijenu a s toga veći broj potencijalnih napadača ima pristup takvoj vrsti tehnologije.

Mjerna jedinica koja se koristi pri mjerenju brzine procesora naziva se FLOPS.23 FLOPS prikazuje broj mjernih uputa u jednoj sekundi. Performanse današnjih računala, odnosno podjela računala po brzini obrade prikazani su u tablici ispod.

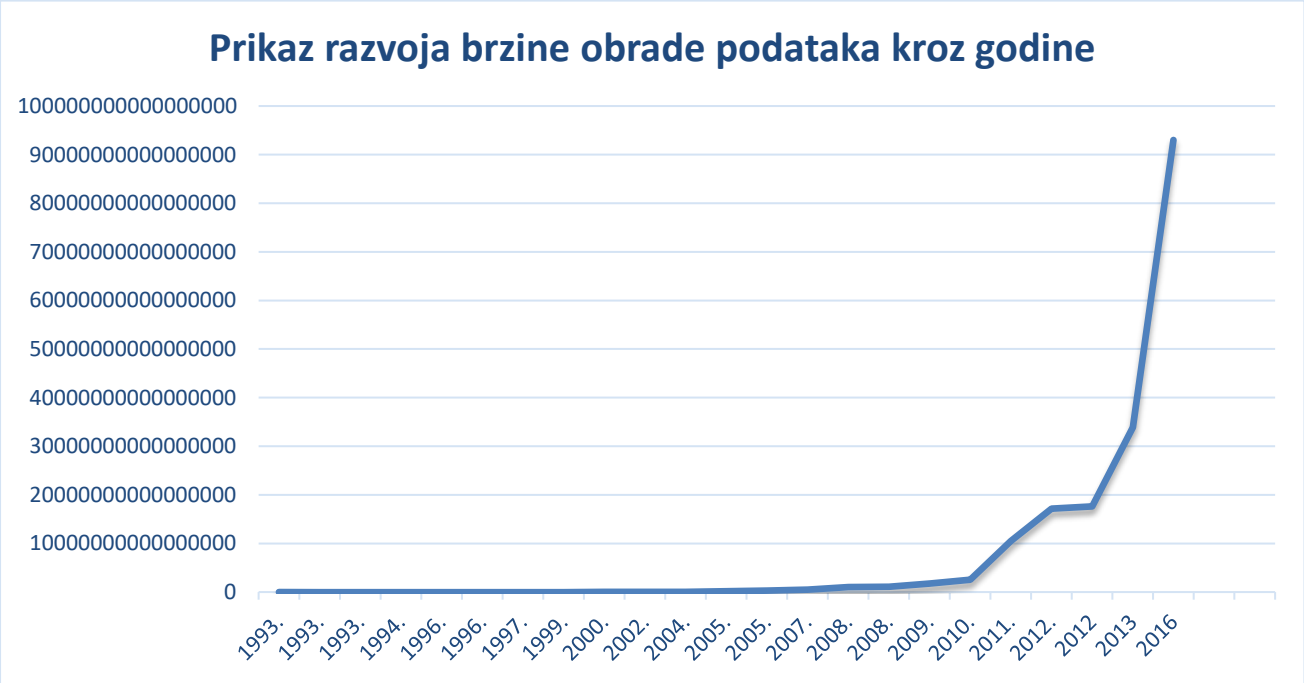
Tablica 2. Brzina obrade podataka

Naziv	Mjerna jedinica	Vrijednost
kiloFLOPS	kFLOPS	10^3
megaFLOPS	MFLOPS	10^6
gigaFLOPS	GFLOPS	10^9
teraFLOPS	TFLOPS	10^{12}
petaFLOPS	PFLOPS	10^{15}

[23] eng. FLoating point OPerations per Second

exaFLOPS	EFLOPS	10^{18}
zettaFLOPS	ZFLOPS	10^{21}
yottaFLOPS	YFLOPS	10^{24}

Slika ispod prikazuje kronološki napredak razvitka računala i super računala po pitanju brzine obrade po podataka. Već početkom 1980-ih brzina se podigla na vrlo visokih 2.4 GFLOPS, brzina značajno raste do 1996. godine a nakon toga dolazi do brzina koje se mjere u teraFLOPS-ima. Nekada su se razlike u brzini osjetile svakih 15 -20 godina koliko je trebalo da dođe do značajnijeg skoka. Današnja superračunala postižu brzinu od nekoliko desetaka petaFLOPS-a.[29]



Slika 1. Kronološki prikaz razvoja brzine obrade podataka u FLOPS-ima kroz godine

Na slici je prikazana brzina u FLOPS-ima u rasponu godina od 1993. do 2016. godine. Prvo super računalo koje je pokazalo velike brzine obrade naziva se Cray-2/8 koji je 1985. godine omogućavao brzinu od 3.9 GFLOPS-a. Superračunalo iz 2016. godine postiže brzine od 93.01 PFLOPS-a a naziva se Sunway TaihuLight. Danas

aktualno superračunalo više ne zauzima cijeli kat zgrade nego je teško nešto manje 17 kg. Trenutno najbrže računalo koristi devetu generaciju Intelovog procesora, napravljen 2017. godine pod nazivom i9, a fascinira entuzijaste svojom snagom. I9 ima 18-jezgreni procesor koji omogućava igranje igrica u 4K kvaliteti a omogućava obradu podataka u teraflops-ima. Takav procesor može bilo koju bazu podataka u Hrvatskoj obraditi u nekoliko sekundi. Cijena takovog procesora iznosi 1999 dolara a težak je nekoliko grama. Da bi nekada prije neko računalo moglo imati te specifikacije moralo je težiti nekoliko tona i zahtijevalo je čitav tim ljudi koji bi upravljani obradom podataka. [31]

4.3. Obrada podataka putem identifikacijske tehnologije

Razvitkom brojnih zemalja sve se češće koriste različiti identifikacijski sustavi. Identifikacijski sustav je sustav koji omogućuje fizički ili daljinski pristup nekom računalnom sustavu, resursima ili Internet servisima. Trend rasta broja takvih sustava u direktnoj je vezi s uporabom visokih tehnologija a i sve većom ponudom digitalnih usluga. Na internetu nema tajnosti i nevidljivosti, svaka osoba je vidljiva na drugačiji način. Zbog neupućenosti korisnika i lažnog osjećaja anonimnosti veliki broj korisnika sam odaje osobne podatke, i to najčešće putem registracije na određene Internet portale. Profiliranje korisnika uključuje rudarenje[24] velike količine podataka koji se prikupljaju pri skladištenju[25] podataka da bi se potom donijeli zaključci o poveznicama između određenih sadržaja. Identifikacija se može osim u komercijalne svrhe vršiti i u svrhe obrane od terorizma, nadzor uporabe i nezakonite distribucije raznih autorskih djela kao što si razni softveri, glazba pa čak i filmovi. Često se profiliranjem može pratiti ponašanje pojedinca za vrijeme njegovog korištenja telekomunikacijskih usluga, kako bi se poduzimale ciljane radnje kao što su personalizirani oglasi.[26] Kod personaliziranih oglasa algoritam prati stranice koje korisnik najčešće posjećuje i na osnovu toga mu se na svakoj stranici nude razne ponude i preporuke.[30]

[24] Rudarenje se u stranoj literaturi još naziva engl. *Data mining*

[25] Skladištenje se još spominje pod nazivom engl. *Data warehousing*

[26]Personalizirani oglasi su oglasi koji se još nazivaju bihevioralno oglašavanje.

4.4. Obrada i prikupljanje prometnih podataka

Europska Unija u svom pravnom okviru osigurava zaštitu prava korisnika koji javno koriste dostupne elektroničke komunkacijske usluge. Prometni podatci su podatci koji sadrže informacije o privatnom životu fizičkih osoba i tiču se prava na poštovanje komunikacije fizičkih osoba ali i određenih skupina pravnih osoba. Prometni podatci se prikupljaju i obrađuju u svrhu obračuna i napalate troškova te u svrhu prijenosa komunikacije. Hrvatki telekom operatori također prikupljaju prometne podatke kako bi mogli vršiti redovnu naplatu SMS-ova, poziva unutar mreže, poziva izvan mreže i sve do nedavno i radi naplate roaminga. Operator mora imati uvid u prostorno kretanje korisnika kako bi znao kada korisnik zove iz Hrvatske ili izvan Hrvatske. Prometni podatci koje svi operateri moraju prikupljati radi pravedne naplate usluga su trajanje poziva, vrijeme poziva, usmjeravanje poziva i mrežu u kojoj započinje i završava poziv. Svi spomenuti podatci se moraju posebno osigurati jer uvid u prometne podatke nekog korisnika pruža detaljan prikaz njegovih navika, aktivnosti to jest kretanja u određenom razdoblju, društvenog života, prikaz osoba s kojima se korisnik druži. [15]

Analiziranjem prometnih podataka može se dobiti uvid u potrošačke sklonosti korisnika, sklonosti sudjelovanja u nagradnim igrama i igrama na sreći, traženje pomoći i savjeta od raznih tarot majstora i slično. Također je moguće dobiti i uvid u intimne probleme korisnika uvidom u pozivanje specijalnih brojeva koji su namjenjeni za pomoć osobaam s psihičkim problemima, osobama sa spolnim bolestima ili osobama s bračnim problemima. Prema Direktivi 2002/58/EZ i članku 6. Jasno su utvrđene obveze operatora javnih komunikacija kako bi se zaštili podatci. Obveza operatera koji je pohranio i obradio podatke je da iste obroše ili ih učini anonimnima u trenutku kada isti više nisu potrebni u svrhu prijenosa komunikacije. [15]

Prema našem zakonu prometni podatci se moraju obrađivati radi obračuna i naplate troškova pružene usluge uz to da operatori smiju obrađivati samo one podatke koji su potrebni za obračun troškova elektroničkih komunikacija ali smao do zastare potraživanja, odnosno do kraja razdoblja tijekom kojeg se račun može zakonski osporiti. Svaki operator je dužan obavijestiti korisnika o obradi podataka i to se

najčešće radi putem općih uvijeta poslovanja operatora, opći uvijeti se nalaze u dokumentaciji koju korisnik potpisuje za vrijeme sklapanja ugovora ili na službenim stranicama operatora. Operatori su kao sigurnosnu mjeru zaštite podataka donjeli pravilo da prometnim podatcma mogu pristupiti samo ovlaštene osobe koje te podatke trebaju radi obračuna troškova, na taj način je smanjen rizik da će netko neovlašten zlouporabiti prikupljene informacije. Osim obračune i naplate prikupljeni podatci se mogu koristiti u svrhu promidžbe, odnosno telefonske prodaje elektroničkih usluga, kao i u svrhu pružanja pojednih posebnih usluga. Da bi se korisniku mogle nuditi razne usluge s dodatnom vrijednošću ili bilo kakva druga vrsta prodaje i promidžbe, potreban je prethodna privola[27] korisnika, odnosno njegov pristanak. Ukoliko je korisnik dao svoj pisani ili usmeni pristanak mogu ga kontaktirati samo ovlaštene osobe koje rade na odjelima telefonske prodaje ili nekog drugog kanala za promidžbu. [15]

4.5. Obrada podataka o lokaciji bez prometnih podataka

Svaki operator mora znati točnu lokaciju mobilnog terminalnog uređaja korisnika i njegov smjer kretanja kako bi mogao točno i kvalitetno pružati elektroničke komunikacijske usluge. Podatci o lokaciji se odnose na geografsku širinu, visinu i duljinu korisnikove terminalne opreme[28], smjer putovanja, identifikaciju mrežne ćelije u kojoj je terminalna oprema smještena u određenom trenutku, kao i na vrijeme kada je podatak o lokaciji zabilježen. Da bi se komunikacija mogla prenijeti između pozivatelja i pozvane strane potrebno je obrađivati podatak o zemljopisnom položaju terminalne opreme korisnika. Iz aspekta propisa o zaštiti osobnih podataka u elektroničkim komunkacijama, u navedenim slučajevima će se podatci o lokaciji smatrati prometnim podatcima, te će se i na njima primjenjivati posebno propisana pravila o dopuštenom prikupljanju i daljnjoj obradi prometnih podataka u pojedine

[27] Privola je dopuštenje, odnosno dozvola koju korisnik daje operatoru

[28] Terminalna oprema je uređaj koji pretvara elektronske impulse u čovjeku razumljivi zvuk i obratno. U ovom slučaju je to mobilni uređaj koji pretvara impulse u zvuk preko zvučnika a u drugom smjeru preko mikrofona pretvara zvuk u impulse pogodne za prijenos putem mreže.

svrhe. U Preporuci Vijeća Europe br.R(95) 4 o zaštiti osobnih podataka u području telekomunikacijskih usluga, s posebnim osvrtom na telefonske usluge iz 1995. godine izrečena je potreba da se podatci o lokaciji bilježe isključivo radi naplate i obračuna troškova za vrijeme korištenja usluga a ne za praćenje kretanja korisnika, utvrđivanaj njhovih identiteta ili utvrđivanja identiteta osoba s kojima komuniciraju. Preporukom je doneseno načelo, prema kojem sustav naplate troškova u trenutku korištenja uređaja nebi smio koristiti toliko preciznu i točnu lokaciju pretplatnika i pozivanih osoba kako se na temelju njih nebi moglo točno locirati sudionike u komunikaciji. Prema našem zakonu temeljno je pravilo da se podatci o lokaciji bez prometnih podataka, koji se odnose na pretplatnike li korisnike javnih komunkacijskih mreža, smiju obrađivati samo ako su anonimizirani, ili uz prethodne privole korisnika. Da bi korisnik mogao dati privolu za korištenje njegovih podataka, u svrhu pružanja usluga dodatne vrijednosti, operator je dužan obavijestiti pretplatnika o vrsti podataka o lokaciji bez prometnih podataka, koji će se obrađivati, o svrsi i trajanju obrade, kao i o tomehoće li se podatci davati nekoj trećoj strani radi pružanja usluga dodatne vriejdnosti. Nakon davanja privole pretplatnik ima pravo u svako doba uskratiti svoju privolu za obradu podataka o lokaciji bez prometnih podataka radi pružanja navedene usluge. Sve vrste privola korisnik ima pravo povući i onemogući na jednostavan i besplatan način, a to pti svakom priključivanju na elektroničku komunikacijsku mrežu ili pri svakom prijenosu komunikacije. U određenim okolnostima neke službe smiju opravdano koristiti podatke o lokaciji bez prometnih podataka bez privole korisnika. To se odnosi na državna tijela i hitnu službu kako bi se mogli odazvati na pozive u hitnim slučajevima. U Zakonu o elektroničkim komunikacijama se, zbog navedenog razloga, propisuje oveza operatora javno dostupnih telefonskih usluga da onemoguće privremeno odbijanje ili izostanak spomenute privole, i tako za svaki pozivni broj nadležnih državnih tijela ili hitnih službi. Iduća iznimka po pitanju obrade podataka bez privole je u slučaju kada takve podatke trebaju tajne službe koje vrše nadzor elektroničkih komunikacija, mreža i usluga. Sve se to opravdava zakonima iz područja nacionalne sigurnosti. U slučaju da tajne službe smatraju kako netko predstavlja opasnost ili može ugroziti nacionalnu sigurnost, imaju pravo locirati ga putem mobilnog uređaja bez suglasnosti, odnosno privolu osumnjičenoga. [15]

5. Opća Uredba o zaštiti podataka - UREDBA (EU) 2016/679

Nakon dugog pregovaranja usvojena je Opća uredba (EU) 2016/679 koja je stupila na snagu 25. svibnja 2016. godine i koja će se primjenjivati u Republici Hrvatskoj od 25. svibnja 2018. godine, za što se već sada provode odgovarajuće pripremne aktivnosti. Uredbom je uvezena obveza voditelja obrade i izvršitelja obrade na čuvanje dokumentacije odnosne na procese obrade za koje su odgovorni, umjesto obveze obavješćivanja nadzornog tijela za zaštitu osobnih podataka koja je propisana člankom 18. i 19. Direktive 95/46/EZ. Ovim promjenama očekuje se smanjenje administrativnih obveza voditelja obrade. S druge strane, uvodi veliki broj novih obveza koje će obrađivati nacionalna samostalna nadzorna tijela[29] i subjekti koji obrađuju podatke. Ističu se sljedećih pet obveza koje se smatraju vrlo bitnima za zaštitu podataka:

1. obvezu voditelja obrade da, prije predviđene obrade podataka koja predstavlja veći stupanj rizika, zatraži od Agencije stručno mišljenje o tome da li je osiguran zadovoljavajući stupanj mjera zaštite,
2. obvezu davanja suglasnosti na sadržaj kodeksa ponašanja odnosnih na zaštitu osobnih podataka slijedom zahtjeva voditelja obrade i drugih subjekata koji obrađuju podatke,
3. obvezu certificiranja određenih procesa obrade kao sigurne,
4. mogućnost sudjelovanja u zajedničkim nadzorima u inozemstvu s drugim nadležnim inozemnim tijelima za zaštitu osobnih podataka, kao i osiguranje takvih nadzora u Hrvatskoj, te

[29] Nacionalno samostalno nadzorno tijelo u Hrvatskoj je Agencija za zaštitu osobnih podataka, poznata pod kraticom AZOP

5. obvezu neposrednog izricanja novčanih kazni za određene povrede odredbi Opće uredbe.

Promjene obuhvaćene Općom uredbom kao rezultat očekuju poboljšanja po pitanju zaštite podataka. Cilj je postići učinkovitiju zaštitu osobnih podataka putem većeg stupnja informiranja subjekata nadležnih za obradu podataka te jačanjem preventivnih sredstava koji stoje Agenciji na raspolaganju pri provođenju Zakona o zaštiti osobnih podataka. Temeljem dosadašnjih iskustava i primjene dobre prakse u provođenju nadzora nad voditeljima obrade Agencija planira nastaviti unaprjeđivati nadzorne aktivnosti. [14]

Sve su promjene i Uredbe donesene zbog razlike u razini zaštite osobnih prava pojedinaca, posebno prava na zaštitu osobnih podataka. Dana 15. prosinca 2015. godine Europski parlament, Vijeće i Komisija postigli su sporazum o novim pravilima zaštite podataka, koji uspostavlja suvremen i usklađen okvir zaštite podataka u zemljama Europske unije. Europski parlament je 27. travnja 2016. godine donio novu regulativu pod nazivom 2016/679 Europskog parlamenta i Vijeća o zaštiti fizičkih osoba u pogledu obrade osobnih podataka. Kao što je već rečeno, nove regulative su donesene većinom radi digitaliziranog i jedinstvenog tržišta, naglog razvoja informatičkih tehnologija te obrade i zaštite podataka koji se koriste u takvom okruženju. Razne telekomunikacijske tehnologije omogućavaju privatnim i pravnim subjektima da koriste osobne podatke bez ograničenja, te im omogućavaju bržu razmjenu, prikupljanje, dijeljenje i obradu podataka. Uz takav napredak tehnologije svi poslovni procesi su posvećeni dobiti, odnosno zaradi, dok s druge strane ti razvoji zahtijevaju snažan okvir zaštite podataka na području Europske unije. Zbog sve većih spoznaja o prisutnosti opasnosti na internetu i povećanja internetskih aktivnosti, cilj Unije je uvesti reformu o zaštitu osobnih podataka. Uz sve navedeno, informacije su postale važan element slobode, a pravo na širenje informacija u velikoj mjeri ovisi o legitimitetima i sposobnostima upravljanja zbirkama podataka. Nakon nešto više od 4 godine rasprave usvojen je novi okvir zaštite osobnih podataka. Nova Uredba se

naziva Opća uredba o zaštiti osobnih podataka (GDPR)[30]. Sredinom prosinca 2015. godine Europski parlament, Vijeće i Komisija postigli su sporazum o novim pravilima zaštite podataka, uspostavljajući usklađen okvir diljem cijele Unije. Dana 8. travnja 2016. godine Vijeće Europe je usvojilo Uredbu i Direktivu a 14. travnja 2016. godine Europski parlament usvojio je Uredbu i Direktivu. Nakon svih obavljenih provjera, dana 4. svibnja objavljeni su službeni tekstovi o Uredbi i Direktivi u Službenom listu EU-a i to na svim službenim jezicima. Nova Uredba stupa na snagu 24. svibnja 2016., a primjenjuje se od 25. svibnja 2018.godine. Donesena je odluka da sve države članice moraju početi primjenjivati novu Direktivu u svome nacionalnom zakonodavstvu do 6. svibnja 2018. godine.

Nova regulativa o zaštiti podataka uključuje:

1. Uredba 2016/679 Europskog Parlamenta i Vijeća od 27. travnja 2016. godine o zaštiti fizičkih osoba glede obrade osobnih podataka i slobodnog kretanja takvih podataka, kojoj se ujedno ukida Direktiva 95/46/EZ.

2. Direktiva 2016/680 Europskog Parlamenta i Vijeća od 27. travnja 2016. godine o zaštiti fizičkih osoba u vezi s obradom osobnih podataka od strane nadležnih tijela u svrhu prevencije, istrage, otkrivanja ili progona krivičnih djela ili izvršenja kaznenih sankcija te o slobodnom kretanju takvih podataka i obavezno ukidanje Okvirne odluke Vijeća 2008/977/JHA. [32][34]

Regulacija o zaštiti podataka vrijedi samo ako se kontrolor podataka ili organizacija ili subjekt podataka[31] temelji u Europskoj Uniji. Promjena u odnosu na dosadašnju Direktivu je da se Uredba također primjenjuje i na organizacije osnovane izvan Europske Unije ako one obrađuju osobne podatke nekog stanovnika Europske Unije. Uredba se ne primjenjuje na obradu osobnih podataka u svrhu nacionalne

[30] General Dana Protection Regulation

[31] Subjekt podataka je osoba čiji se podatci obrađuju

sigurnosne djelatnosti ili za provedbu zakona[32]. Prema Europskoj Komisiji osobni podaci su sve informacije koje se odnose na pojedinca, na privatnom, profesionalnom ili javnom životu. Prema novoj Regulativi osobni podatak može biti gotovo svaki podatak o nekoj osobi, ime, fotografije, adresa e-pošte, bankovni podatci, postovi na društvenim stranicama pa čak i medicinske informacije ili IP adresa računala. [32][34]

Europska uredba o zaštiti podataka sadrži sljedeće ključne promjene:

- Jedinstveni pravilnik će se primjenjivati na sve države članice EU[33]
- Svaka država članica će uspostaviti neovisno nadzorno tijelo za saslušavanje i ispitivanje pritužbi i sankcioniranje administrativnih prekršaja i slično
- Ako se poslovanje odvija na više lokacija u EU, odnosno u više objekata, imat će jedinstveno nadzorno tijelo kao svoju glavnu upravu u kojoj se obavljaju glavne djelatnosti
- Nadležno tijelo će djelovati kao jedno kako bi nadgledalo sve prerađivačke djelatnosti tog poslovanja diljem EU
- Europski odbor za zaštitu podataka će koordinirati Nadzorno tijelo
- Postoje i izuzeci za podatke koji se obrađuju u kontekstu zapošljavanja i podatke koji se obrađuju u svrhu nacionalne sigurnosti, a koji još uvijek mogu biti podložni pojedinačnim propisima zemlje (članci 2. stavak 2. točka a) i članak 82. stavak Opće uredbe o zaštiti osobnih podataka) [32][34]

Svi zahtjevi za obavijesti moraju sadržavati vrijeme zadržavanja za osobne podatke i kontakt podatke za kontrolora podataka i službenika za zaštitu osobnih podataka. Građani po novom imaju pravo postavljati pitanja i boriti se za odluke koje se često tiču onih koji su dobiveni algoritmima. Prema članku 25. zadano je da

---

[32] Pod pojmom provedba zakona smatraju se djelatnosti nadležnih tijela u svrhu prevencije, istrage, otkrivanja ili progona kaznenih djela ili izvršenja kaznenih sankcija

[33] Europska Unija

privatnost po dizajnu zahtjeva da se zaštita podataka osmišljava u razvoju poslovnih procesa za sve proizvode i usluge. Po članku 35. procjene utjecaja na zaštitu podataka moraju se provoditi kada se pojave specifični rizici za prava i slobode nositelja podataka. Službenici za zaštitu podataka moraju osigurati usklađenost unutar organizacija.

Više se pozornosti obraća i na suglasnost subjekata. Potvrda pristanka mora biti izričita za prikupljanje podataka i svrhu zbog kojih se podatci prikupljaju. Za svu djecu mlađu od 16 godina roditelji ili skrbnik djeteta mora dati suglasnost i dozvolu za obradu podataka. Kontrolori podataka moraju biti u stanju dokazati pristanak, odnosno suglasnost, i omogućiti povlačenje suglasnosti. [32][33][34]

U okviru Uredbe, nezavisni službenik za zaštitu podataka bit će pod zakonskom obvezom da obavijesti Nadzorno Tijelo[34] bez pretjeranog kašnjenja, to je i dalje predmet pregovaranja. Izvještavanje o kršenju podataka ne podliježe standardima i vjerojatno će novom Uredbom biti predviđeno da se takva kršenja moraju prijaviti Nadzornom Tijelu čim postanu svjesni kršenja podataka, ta tema je obrađena u članku 31. Iz članka 32. može se vidjeti da je potrebno obavijestiti pojedince ako se utvrdi nepovoljan utjecaj na njih.

GDPR[35] uvodi sankcije ukoliko se netko ne bi pridržavao pravila. Kazne se mogu izreći u slučaju kršenja odredbi, iste mogu biti u iznosu do 10 000 000 Eura ili u slučaju poduzetnika do 2% ukupnog godišnjeg prometa na svjetskoj razini za prethodnu financijsku godinu ovisno o tome što je veće. Za kršenja odredaba iz članka 83. stavka 5. mogu se izreći novčane kazne u iznosu do 20 000 000 Eura, ili u slučaju poduzetnika do 4% ukupnog godišnjeg prometa na svjetskoj razini za prethodnu financijsku godinu.

Takozvano pravo zaboravljanja, ili pravo na brisanje, zamijenjeno je pograničnijim pravom na brisanje u verziji GDPR-a koju je usvojio Europski parlament u ožujku 2014.

---

[34] Eng.Supervisory Authority

[35] Eng.Global Data Protection Regulation

članak 17. predviđa da subjekt podataka ima pravo zatražiti brisanje osobnih podataka koji se odnose na njega na bilo koji od brojnih razloga, uključujući nepoštivanje čl. 6.1 (zakonitost) koji uključuje slučaj (f) ako su legitimni interesi kontrolor nadjačava interesi ili temeljna prava i slobode nositelja podataka koji zahtijevaju zaštitu osobnih podataka.

Još jedna bitna stavka na koju treba obratiti pozornost je prenosivost osobnih podataka. Osoba mora moći prenijeti svoje osobne podatke iz jednog elektroničkog sustava obrade u drugi, a da ih kontrolor podataka ne onemogući. Nadalje, podatke mora dati kontrolor u strukturiranom i uobičajenom elektroničkom obliku. Pravo na prenosivost podataka pruža članak 18. GDPR-a. [32][34]

6. Primjena Opće Uredbe u praksi

Zbog brzog tehnološkog razvoja i globalizacije pojavili su se novi izazovi u zaštiti osobnih podataka. Opseg prikupljanja i razmjene osobnih podataka značajno se povećava. Tehnologijom se privatnim društvima i tijelima javne vlasti omogućuje uporaba osobnih podataka u dosada nedosegnutom opsegu radi ostvarenja njihovih djelatnosti. Pojedinci svoje osobne informacije sve više čine dostupnima javno i globalno. Radi sprečavanja stvaranja ozbiljnog rizika zaobilaženja propisa, zaštita pojedinaca trebala bi biti tehnološki neutralna i ne bi smjela ovisiti o upotrebljavanim tehnologijama. Zaštita pojedinca se odnosi na automatsku i ručnu obradu podataka. Bitno je naglasiti da se nova Uredba ne primjenjuje na osobne podatke preminulih osoba. Obrada osobnih podataka u svrhe različite od svrha za koje su podaci prvotno prikupljeni smjela bi se dopustiti samo ako je obrada usklađena sa svrhama za koje su osobni podaci prvotno prikupljeni. U takvom slučaju nije potrebna pravna osnova zasebna od one kojom je dopušteno prikupljanje osobnih podataka. Ako je obrada potrebna za obavljanje zadaće koja se obavlja u javnom interesu ili pri izvršavanju službene ovlasti koju ima voditelj obrade, pravom Unije ili pravom države članice mogu se utvrditi i odrediti zadaće i svrhe za koje će se nastavak obrade smatrati usklađenim i zakonitim. [34]

Prema članku 6. obrada podataka je zakonita samo ako je ispitanik dao privolu za obradu svojih osobnih podataka u jednu ili više svrha, ako je obrada nužna kako bi se zaštitili ključni interesi ispitanika i slično. U praksi nitko ne smije osobne podatke ispitanika koristiti i obrađivati ako ispitanik osobno nije dao dopuštenje za takvu obradu. U slučaju da pojedinac da svoje podatke za vrijeme nekog anketiranja, anketar ne smije te podatke dati nekoj firmi ili nekoj trećoj osobi ako nema dopuštenje od vlasnika podataka.

U slučaju da pojedinac napravi neko kazneno djelo ili ima neku kaznenu osudu, zbog mjera sigurnosti, nadzorno službeno tijelo smije obrađivati podatke jer je to tako odobreno pravom Unije. Obrada osobnih podataka koji se odnose na kaznene osude i kažnjiva djela ili povezane mjere sigurnosti na temelju članka 6. stavka 1. provodi se samo pod nadzorom službenog tijela. (članak 10.) U slučaju da pojedinac opljačka

poslovnicu neke banke, pravosudna tijela imaju pravo obrađivati njegove podatke bez znanja i bez pristanka.

U slučaju da voditelj obrade prikuplja osobne podatke ispitanika, dužan je ispitanika upoznati sa informacijama kao što su:

- identitet i kontakt podatci voditelja obrade
- svrhu obrade radi kojih se podatci prikupljaju i upotrebljavaju

Prema članku 13. ako netko vrši prikupljanje podataka u javnosti putem anketiranja dužan je obavijestiti ispitanika u koju svrhu se prikupljaju podatci i kako će se upotrebljavati, isto tako je potrebno ispitaniku dati i kontakt podatke voditelja obrade. U slučaju da ispitanik ne želi da se njegovi podatci u budućnosti obrađuju ima pravo nazvati voditelja obrade i pozvati se na pravo zaborava.

Članak 15. kaže da ispitanik ima pravo dobiti od voditelja obrade potvrdu obrađuju li se osobni podaci koji se odnose na njega te ako se takvi osobni podaci obrađuju, pristup osobnim podacima i informacijama kao što su, svrha obrade, kategorije osobnih podataka o kojima je riječ, ako se osobni podaci ne prikupljaju od ispitanika, svakoj dostupnoj informaciji o njihovu izvoru i drugi.

Gore spomenuto pravo na zaborav se još naziva pravo na brisanje (članak 17.) U slučaju da ispitanik želi zabraniti obradu svojih podataka, potrebno voditelj obrade ima obvezu obrisati osobne podatke bez nepotrebnog odgađanja ako je ispunjen jedan od uvjeta:

- Podatci više nisu nužni u odnosu na svrhe za koje su prikupljeni
- Ispitanik uloži prigovor na obradu u skladu s pravom na prigovor iz članka 21 stavka 1.

Doc.dr.sc. Marija Boban, je na okruglom stolu pojasnila primjenu osobnog podatka u praksi, pomoći primjera iz svakodnevnice:

„Objava slike na nekoj mreži je osobni podatak u slučaju da uz sliku piše ime i prezime osobe koja je sliku objavila. Ukoliko osoba nije označena to nije osobni podatak“;

Doc.dr.sc. Marija Boban, također se dotakla problema u kojem se biometrijski podatak ne smatra osobnim a jedinstven je kod svakog pojedinca.

„Do sada u Hrvatskoj nismo imali biometrijske podatke kao osobne podatke, niti smo imali dio zakona kojim se to uređuje ili regulira. Ne može biti osobnog podatka koji može biti veći od zjenice oka ili otiska prsta, a velika većina organizacija baš to koristi kao zaštitu podataka, imamo još dosta rupa u zakonu. Ovo je dobra prilika da bi taj dio uredili.“ [36]

Danas je nemoguće obrisati podatke s interneta moguće je samo maknuti poveznice na googlu. Što znači da ako vi u praksi zatražite brisanje podataka s interneta, oni neće biti obrisani samo se neće prikazivati u google pretraživaču.

„Problem je što postoji matica googla, ali i google.hr i slično, ali nikada se podatak s interneta neće potpuno izbrisati, ne postoji takav način. Ali možete zabraniti daljnju obradu podataka.“ [36]

Potrebno je početi primjenjivati novu uredbu u što većoj mjeri zbog rapidnog razvoja tehnologije, te teme se na okrugom stolu FSec-a dotaknuo doc.dr.sc.Goran Vojković.

„Stara Direktiva je bila iz 1995. godine, tada su brzi modemi išli 2400 moda, pa ste morali preko telefona zvati drugu državu gdje nikome nije palo napamet bazu podataka prenijeti telefonski nego se sve skidalo na diskete i prenosilo. A u današnje vrijeme novi Intelov procesor 1999 dolara je maloprodajna cijena, a zamjenjuje superračunala prije 10 godina. Može se na jednom kućnom računalu stvoriti nevjerojatno jaka i opaka i opasna baza svih građana Republike Hrvatske s adresama, običajima i podatcima.“[37]

GDPR donosi vrlo visoke kazne i država ih ne može ne odabrati i neće moći nekoga manje kažnjavati. Kazna je npr. 20.000.000 eura, ili 4% prometa, ovisi što je veće. Ukoliko neka osiguravajuća kuća proda podatke svojih 10.000 osiguranika, a nije smjela, onda će nadzorno tijelo (u Hrvatskoj AZOP) utvrditi da je prosječna vrijednost povrede 1.000 kuna po osiguraniku. U tom slučaju kazna bi bila umnožak

prosječne povrede i broja osiguranika. U slučaju ovog primjera iznos kazne bi bio 10.000 x 1000 = 10.000.000 kuna.

Pravo zaborava bi se moglo krivo protumačiti s ciljem zlouporabe. Ukoliko pojedinac nekom operateru duguje iznos od 500 kuna, isti taj pojedinac neće moći tražiti zaborav ili brisanje svojih podataka, jer bi u tom slučaju njegov dug nestao.

Članak 99. Uredbe kaže da ova uredba stupa na snagu dvadesetog dana od dana objave o u Službenom listu Europske unije, a primjenjuje se od 25. svibnja 2018. godine.

7. Dionici primjene- poznavanje (anketa)

Korištenje tehnologije i usluga javne telekomunikacijske mreže korisnicima je bitno zbog usluga koje takva mreža pruža. Prednost te mreže je mogućnost mobilnosti, povezivanja i omogućavanja dijeljenja podataka među korisnicima. Svakom korisniku je bitno da se može slobodno kretati, obavljati svakodnevne obaveze poslovnog ili privatnog karaktera te uvijek biti dostupan u telekomunikacijskom sustavu.

S obzirom da se podatci koriste, netko te podatke mora unaprijed prikupiti, pohraniti, obraditi i osigurati prijenos istih. Svi koji su u dodiru sa osobnim podatcima moraju s njima postupati prema zakonu kako je propisano raznim direktivama i uredbama, u protivnom slijede velike kazne.

7.1. Struktura anketnog upitnika o važnosti zaštite osobnih podataka

U svrhu stjecanja predodžbe o informiranosti korisnika telekomunikacijskih mreža o poznavanju novih propisa o zaštiti osobnih podataka unutar Europske unije.

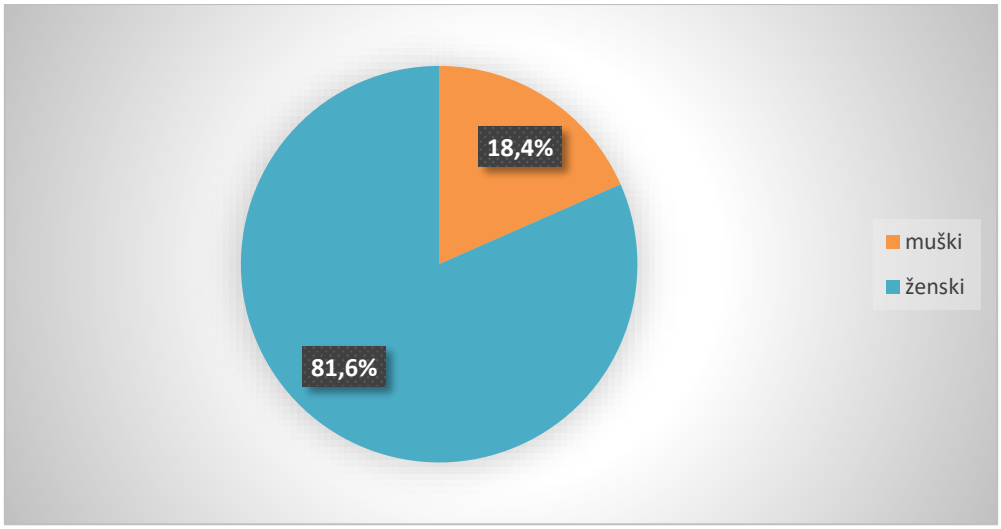
Anketa je nastala u okviru diplomskog rada na Fakultetu prometnih znanosti u Zagrebu s ciljem dobivanja informacija o poznavanju Europske Direktive 2016/679 za sve korisnike javne telekomunikacijske mreže. Anketa se sastoji od 22 pitanja, koja su navedena u Prilogu I ovog rada, s unaprijed ponuđenim odgovorima kako bi se olakšalo ispitivanje korisnika i ujedno skratilo vrijeme potrebno za uspješnim rješavanjem iste. Anketnom istraživanju je pristupilo 680 ispitanika, što je zadovoljavajući broj pristupnika anketi s obzirom na temu i područje provedenog istraživanja. Ciljana skupina korisnika bila je u starosnoj dobi od 18 do 65 godina te prema izračunu broja stanovnika preuzetoga iz Državnog zavoda za statistiku Republike Hrvatske broj ciljane skupine iznosio je 2.586 895 stanovnika.[39]

Dovoljan broj ispunjenih anketnih upitnika za relevantnost rezultata same ankete izračunat je putem “Raosoft – Simpe size calculator” te je potreban broj

ispunjenih anketa iznosio 385 anketa, s time da je dobiveni broj izračunat sa 95% točnosti i razine dopuštene pogreške od 5%. [40]

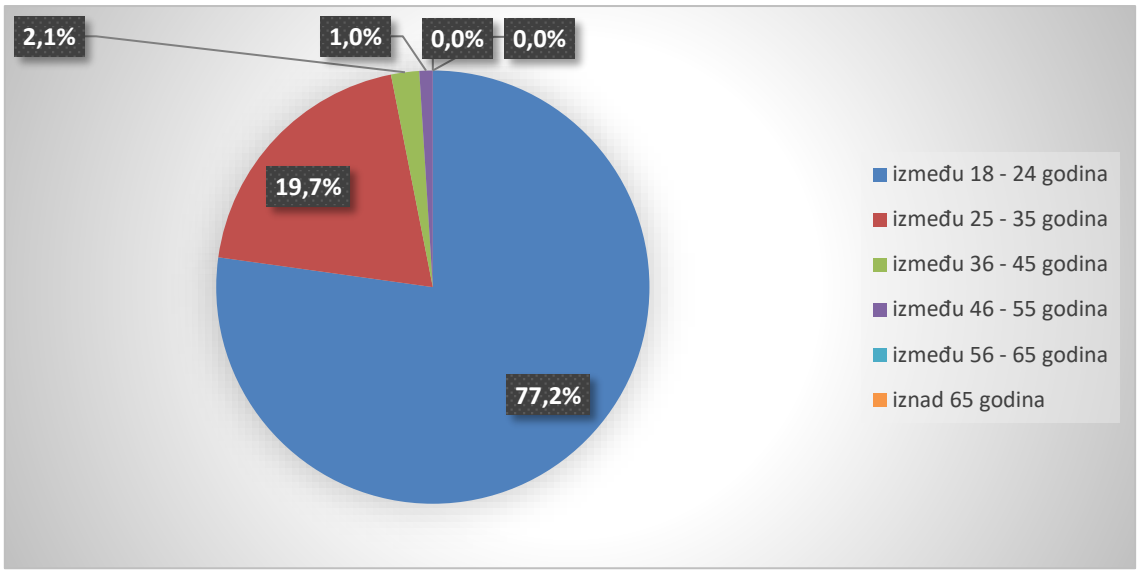
7.2. Obrada anketnog upitnika na temelju predanih odgovora

Ispitanici su najprije pitani o pripadnosti spolu. Svrha pitanja bila je dobiti informaciju o tome jesu li bolje informirani pripadnici muškog spola ili pripadnice ženskog spola. Iz grafikona 1., vidljivo je kako je anketi pristupilo više osoba muškog spola u odnosu na ženski spol. Izraženo u postotcima, anketi je pristupilo 81,6 % osoba ženskog spola te 18,4 % osoba muškog spola.



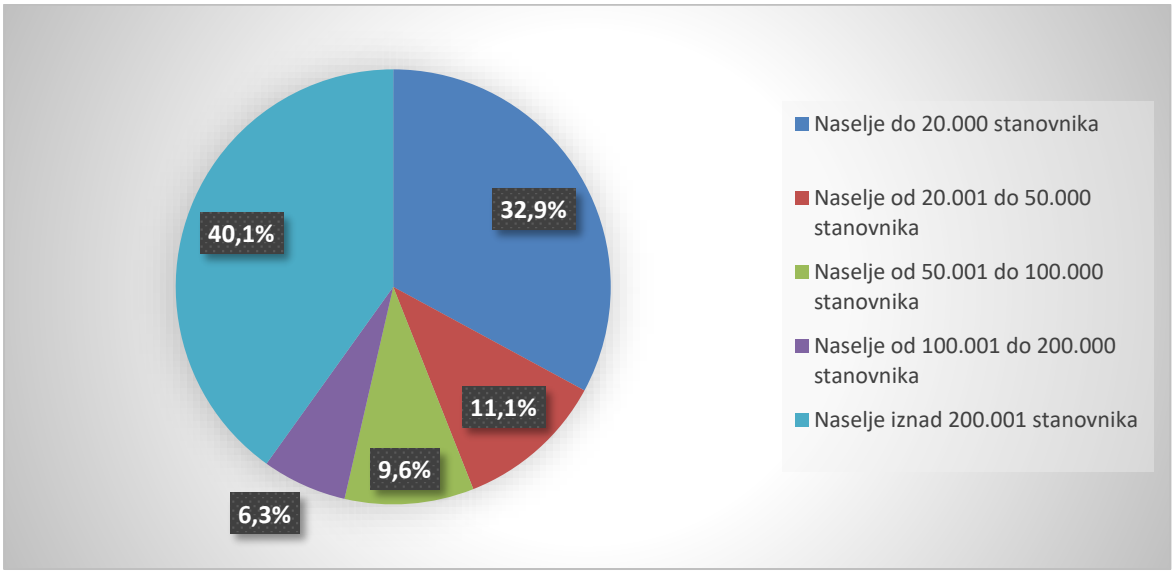
Grafikon 1. Spolna struktura ispitanika

Nakon toga ispitanike se pitalo kojoj dobnoj skupini pripadaju. Ponuđeni odgovori na ovo pitanje su bile kategorije dobnih skupina. Prema predanim odgovorima ispitanika, moguće je zaključiti kako su anketi pristupili uglavnom mlađi ispitanici i ispitanici zrelije dobi, pretežno dobne skupine od 18 do 35 godina. Najbrojnija dobna je skupina mladih ispitanika, točnije 77,2 % vidljivo na grafikonu 2.



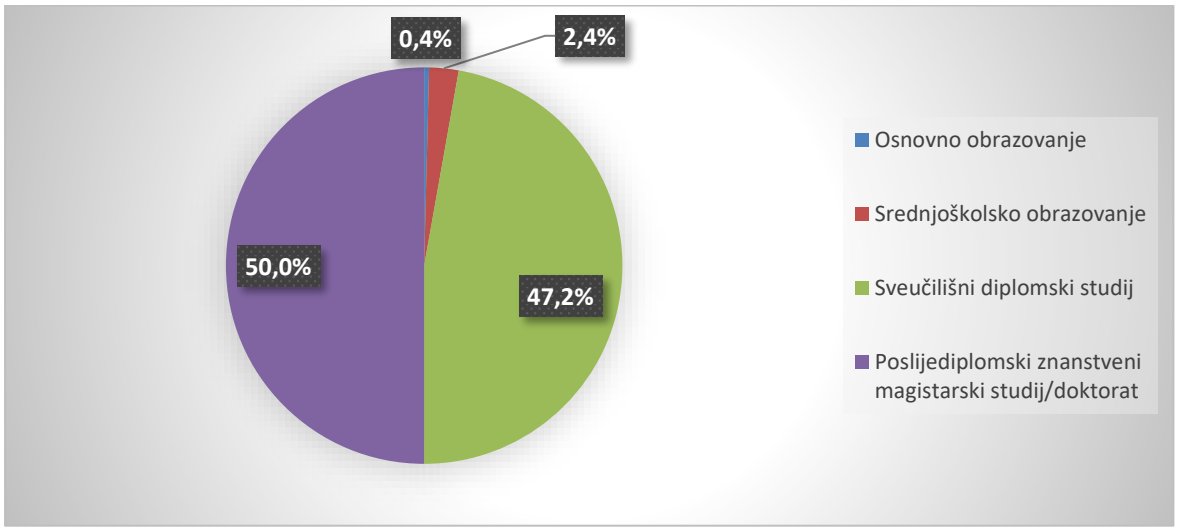
Grafikon 2. Dobna skupina ispitanika

Idućim pitanjem smo dobili uvid u veličinu naselja u kojem ispitanici žive. Iz grafikona 3. možemo vidjeti da najveći broj ispitanika dolazi iz većih sredina, što znači da im je stalo do važnosti zaštite podataka jer uz ubrzan tempo života u većim sredinama imaju vremena i volje odgovoriti na sva pitanja iz ankete.



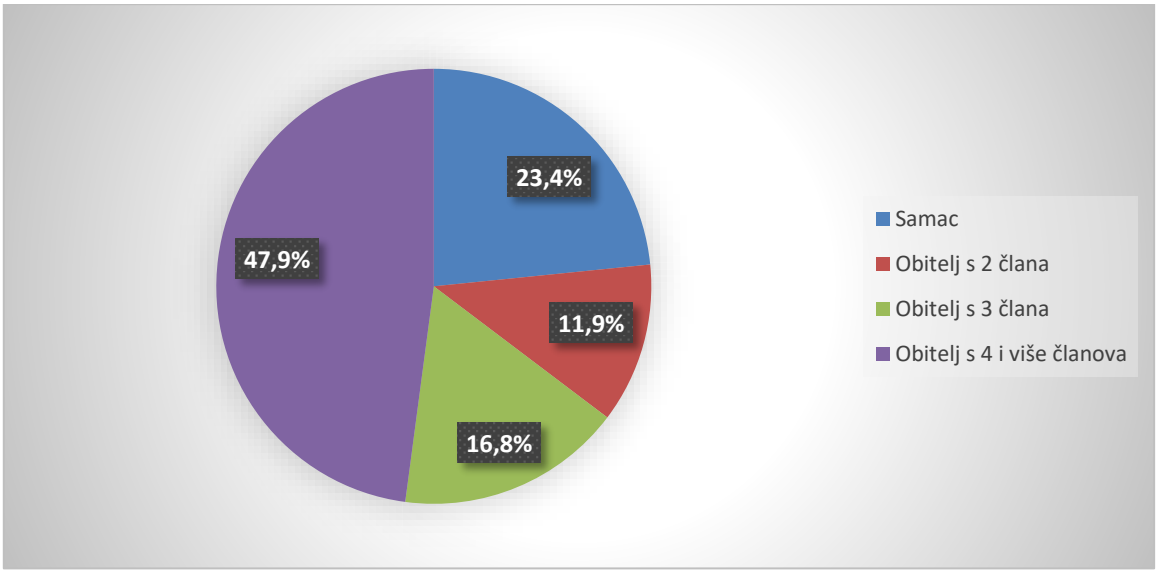
Grafikon 3. Veličina naselja u kojem žive ispitanici

Grafikon 4. nam prikazuje stručnu spremu ispitanika, iz čega je vidljivo da je preko 97% ispitanih ima završen fakultet ili studiraju na nekom sveučilištu. Moglo bi se reći da su obrazovaniji ljudi svjesniji opasnosti koje vrebaju na internetu.



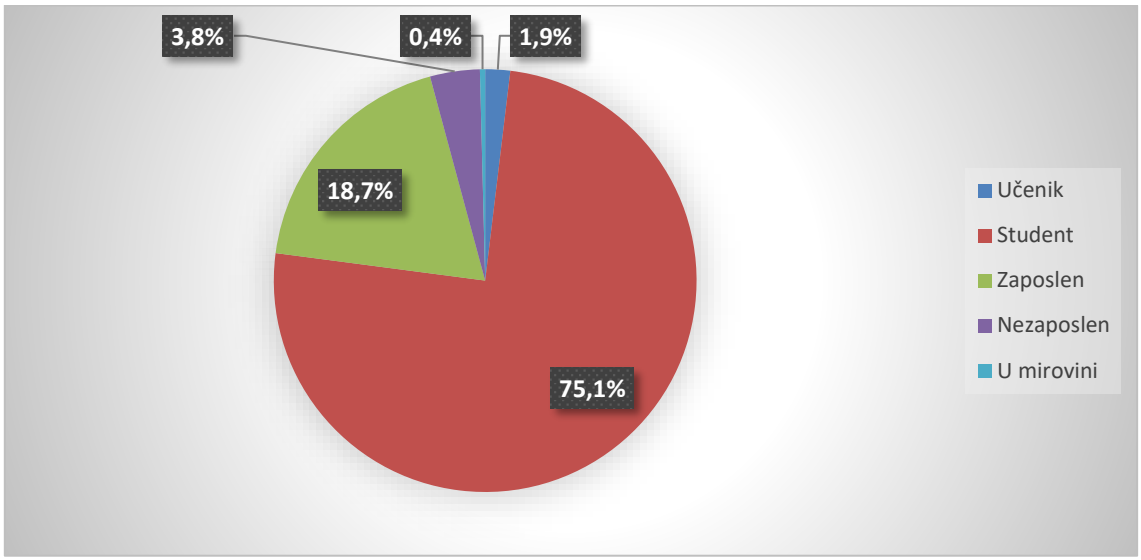
Grafikon 4. Stručna sprema ispitanika

Grafikon ispod se odnosi na brojno stanje u kućanstvu. Iz grafikona je vidljivo da preko 60% ispitanika živi u obiteljima sa dva ili više članova, dok samo 23,4% ispitanika žive kao samci.



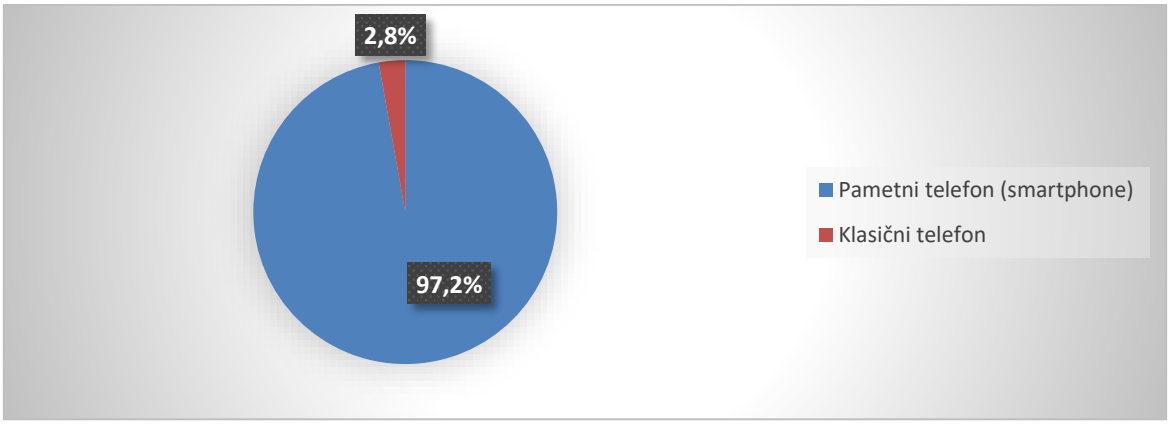
Grafikon 5. Broj članova u obitelji

Iz grafikona 6. dobiven je uvid u zanimanje ispitanika. Spajanjem rezultata ovog grafa i idućih pitanja dobili smo točan uvid u količinu stečenog znanja kod studenta u Republici Hrvatskoj po pitanju važnosti zaštite osobnih podataka.



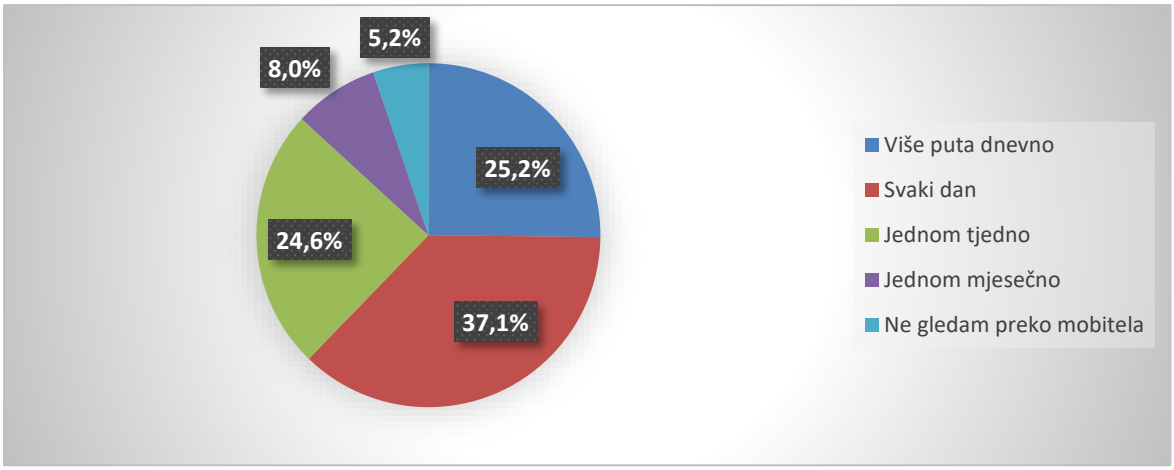
Grafikon 6. Zanimanje ispitanika

U današnje vrijeme kada se tehnologije vrlo brzo razvijaju bitno je znati koliki postotak ispitanika koristi klasične mobitele na tipke, a koliki postotak ispitanika koristi mobitele na ekran s dodirom, eng. *touch.* Iz ankete ovih 2.8% ispitanika su sigurni da neće putem mobitela otkriti svoje podatke, ili da će se namjerno ili nenamjerno registrirati na nekim stranicama putem mobilnog uređaja i tako izložiti svoje osobne podatke nekome tko ih može zloupotrijebiti.



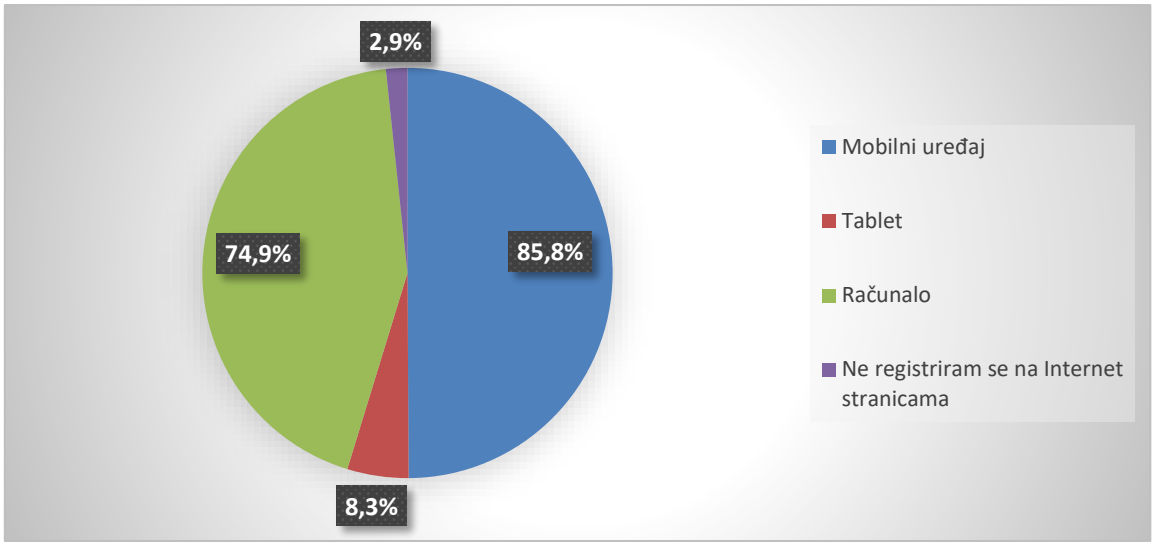
Grafikon 7. Vrsta mobilnog uređaja

Grafikon 8. prikazuje učestalost provjere elektronske pošte putem mobilnih uređaja. Jasno je vidljivo da 62,3% ispitanika pregledava mailove svaki dan, što uvelike povećava opasnost za osobne podatke. Mailom se mogu poslati razni virusi ili zlonamjerne poveznice koje traže potvrdu lozinke ili neku vrstu registracije.



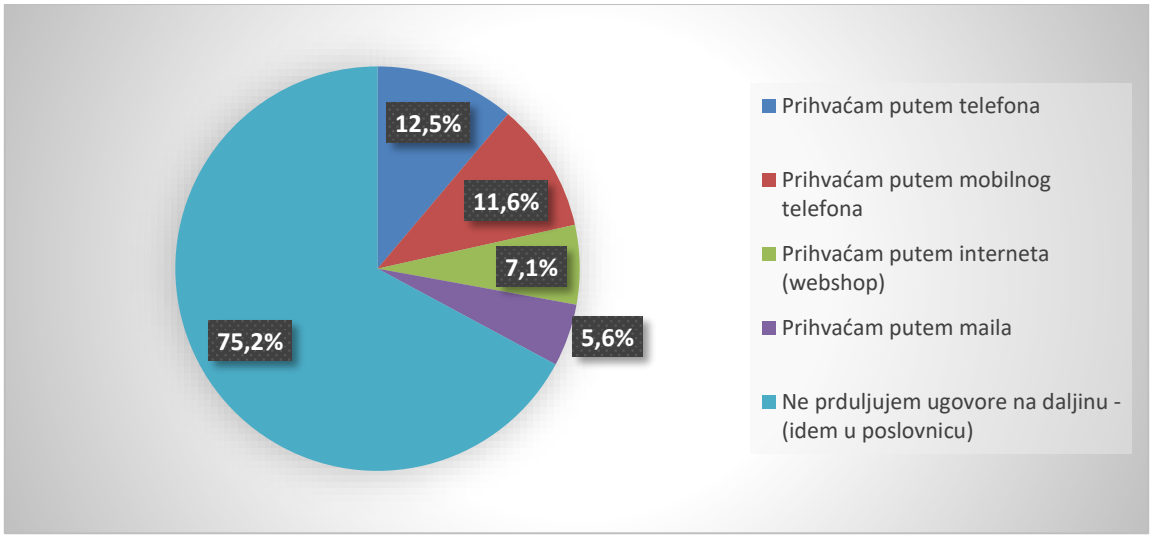
Grafikon 8. Učestalost pregledavanja elektronske pošte

Grafikon 9. prikazuje odgovor na pitanje kojim se sve uređajima ispitanici registriraju na Internet stranicama i raznim portalima. Pošto većina ispitanika koristi računala, tablete a gotovo svi imaju pametne telefone, na ovo pitanje moglo odgovoriti s više odgovora. Prema rezultatima ankete može se vidjeti da većina ispitanika osobne podatke unosi putem mobilnih uređaja i računala.



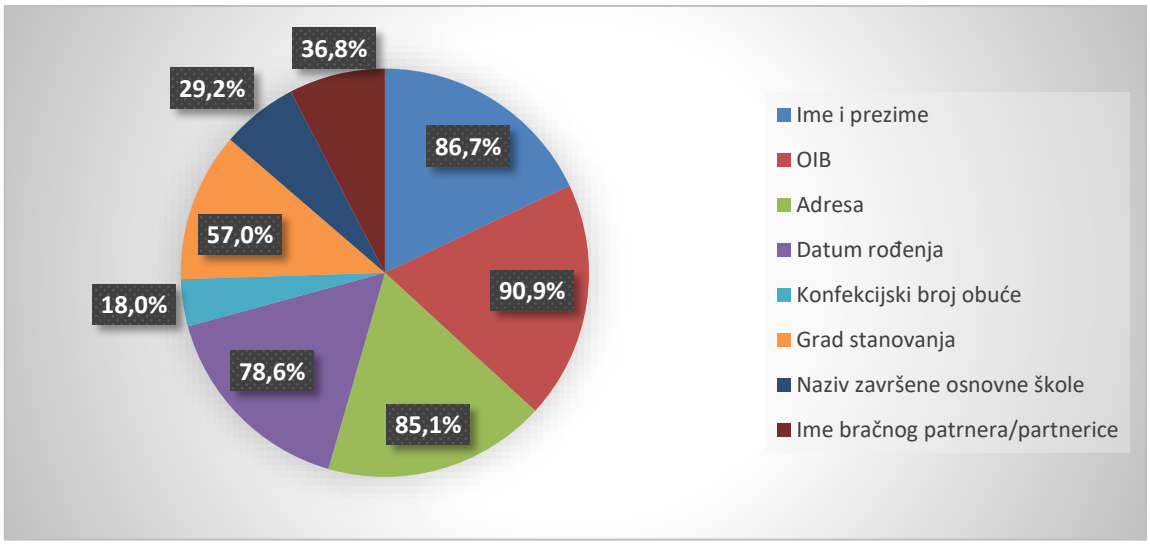
Grafikon 9. Uređaji kojima se korisnici registriraju na mreži

Povećanjem broja usluga koje nude telekom operateri raste i ponuda prema krajnjim korisnicima. Operateri na sve načine pokušavaju povećati prihode i korisnicima pružiti što više usluga. Najviše prodaja novih usluga ili produljivanja dosadašnjih usluga događa se putem telefona ili putem mobilnog uređaja. Rezultat takve produktivnosti je jednostavnost, sve se može odraditi „od doma“, bez odlaska u razne poslovnice i čekanja čak do sat vremena na red. Najava snimanja svakog poziva je urodila povjerenjem i osjećajem sigurnosti, što se najbolje vidi iz grafikona 10.



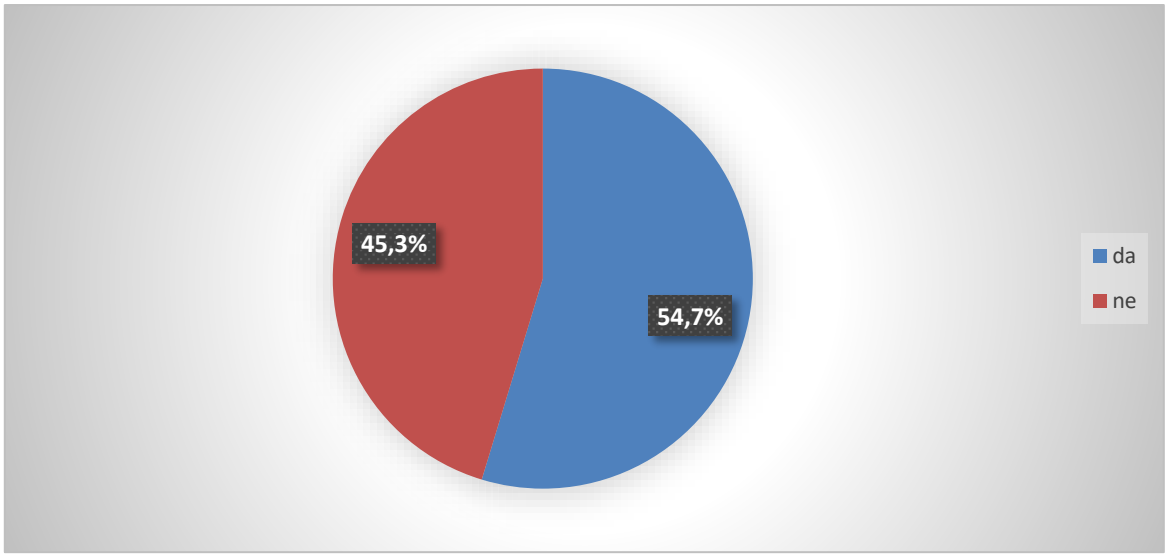
Grafikon 10. Načini sklapanja ugovora s operaterima

Osobni podatak je poznati pojam ali mali broj ispitanika stvarno zna što je osobni podatak; vidljivo na Grafikonu 11. Gotovo 91% ispitanika misli da je OIB osobni podatak, što i je točno. Osobni podatak je svaki podatak pomoći kojeg se može identificirati neku osobu, tako da svaki ponuđeni odgovor u nekom kontekstu može biti osobni podatak.



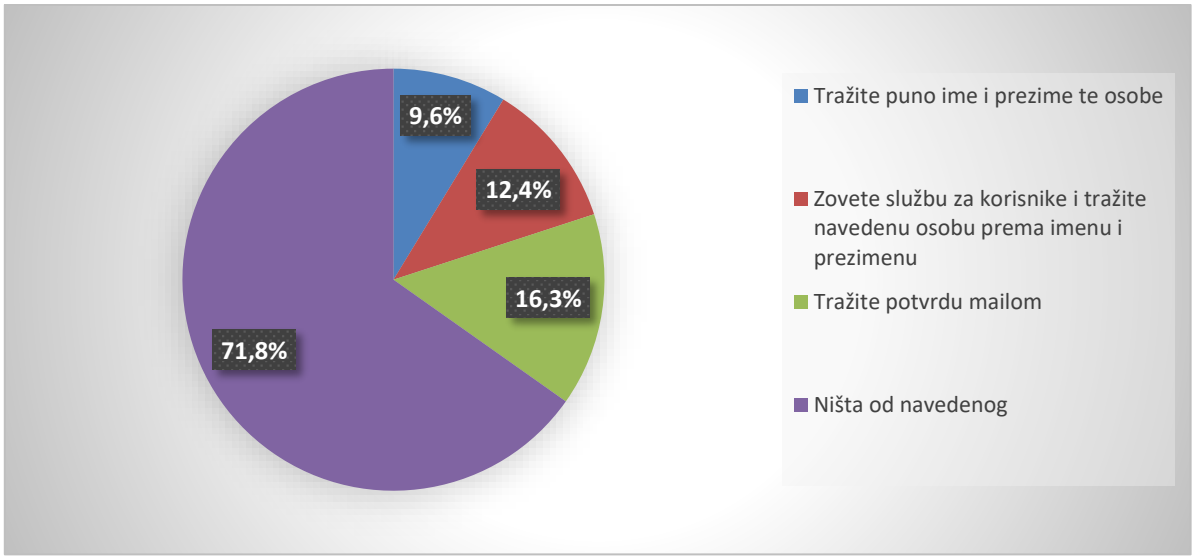
Grafikon 11. Odgovori na anketno pitanje "Što je osobni podatak?"

Gledajući televizijske emisije poput Potrošačkog koda i Provjerenog, kod ispitanika se probudila svijest o posljedicama koje nastaju prilikom raznih pokušaja prevara. Zbog medija koji upozoravaju korisnike o opasnostima, kod korisnika se počela javljati sumnja te samo 54,7% ispitanika vjeruje da se s druge strane slušalice stvarno nalazi zaposlenih telekom operatera. Vidljivo na grafikonu 12.



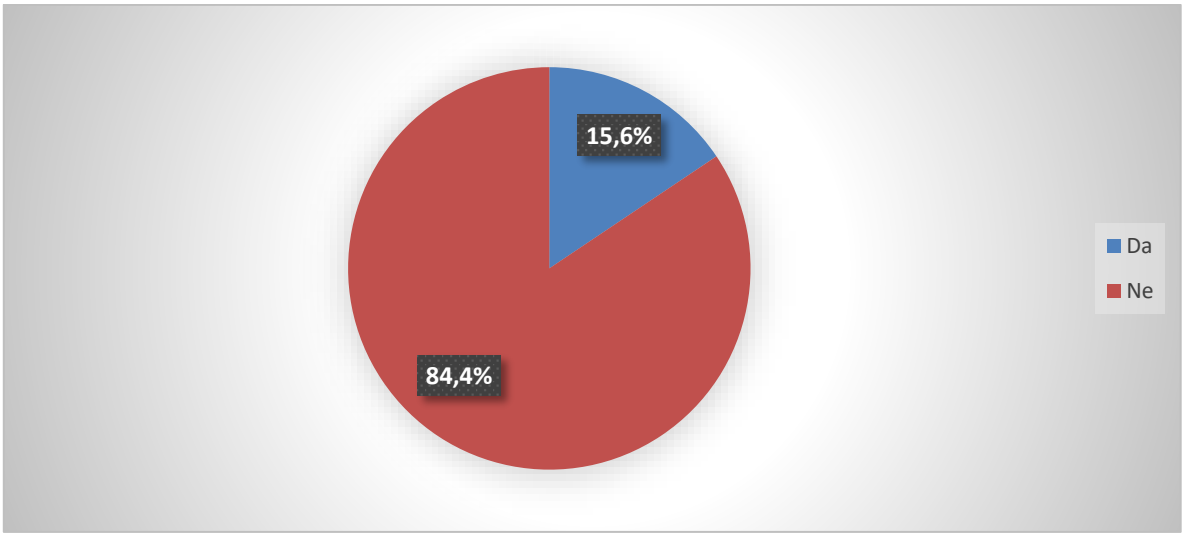
Grafikon 12. Odgovor na anketno pitanje "Vjerujete li da se osoba koja Vas nazove ne predstavlja lažno?"

Grafikon 13. prikazuje neke od načina na koje ispitanici vrše identifikaciju osoba koje ih kontaktiraju i predstavljaju se kao zaposlenici telekom operatera. U 71.8% ispitanika spadaju svi koji ne pristaju na ugovore putem telefona, koji ne vrše identifikaciju i oni koji imaju neki od svojih načina provjere osobe s kojom razgovaraju.



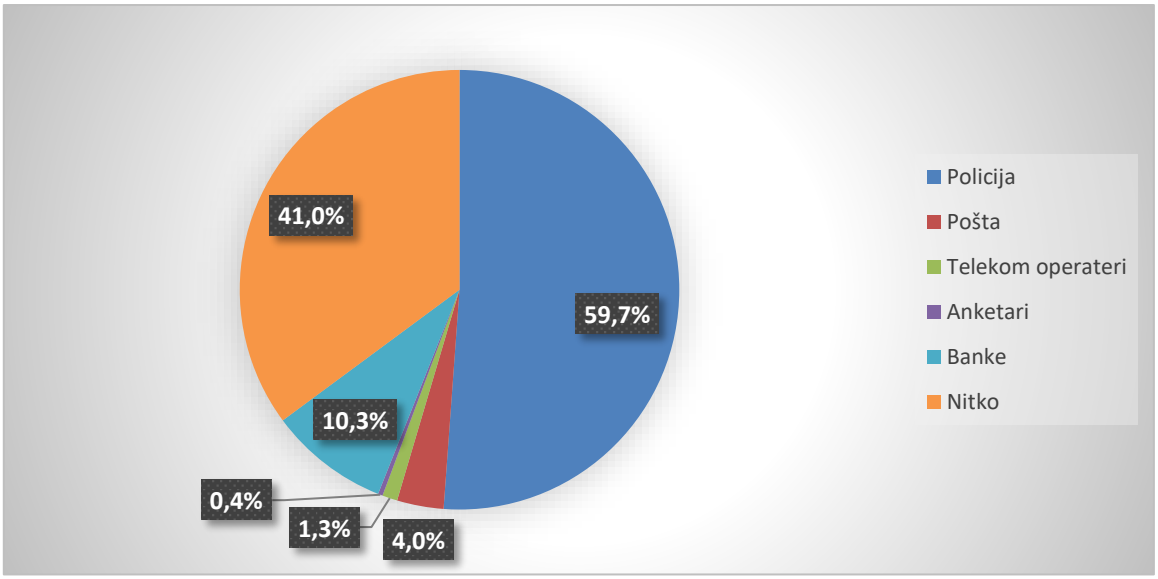
Grafikon 13. Načini na koje ispitanici vrše identifikaciju osoba koje ih zovi i predstavljaju se kao telekom operateri

Iz grafikona 14. se vidi svijest ispitanika o opasnostima koje mogu nastati ukoliko nekome pošalju svoju osobnu iskaznicu. Ukoliko preslika osobne iskaznice završi kod nekoga tko ima loše namjere, postoji mogućnost da dođe do krađe identiteta.



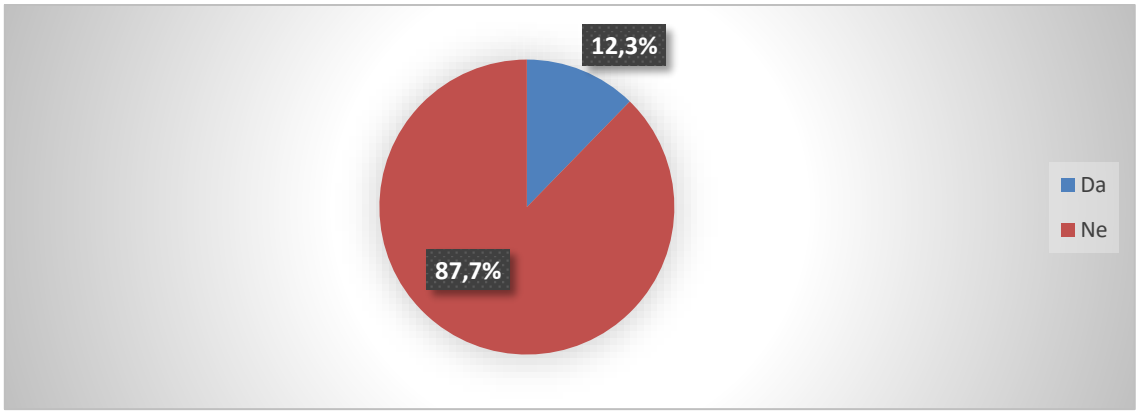
Grafikon 14. Prikaz anketnog odgovora na pitanje "Šaljete li presliku osobne iskaznice mailom?"

Grafikon 15. prikazuje odgovor na anketno pitanje „Tko smije obrađivati Vaše osobne podatke bez Vašeg znanja?“. 59,7 % ispitanika misli da policija ima pravo obrađivati osobne podatke pojedinaca bez njegovog znanja. U pravilu nitko ne smije prikupljati, obrađivati i dijeliti osobne podatke bez da se vlasniku jasno da do znanja zbog čega se podatci prikupljaju, osim ako nije zakonski drugačije regulirano.



Grafikon 15. Prikaz odgovora na anketno pitanje "Tko smije koristiti Vaše osobne podatke bez Vašeg znanja?"

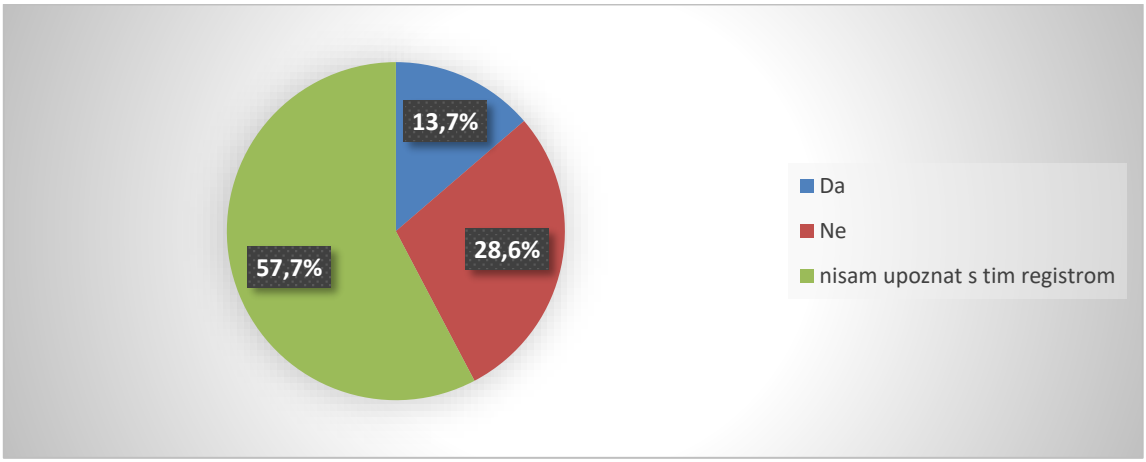
Iz grafikona 16. vidljivo je da samo 12,3% ispitanika zna da postoji pravo zaborava. Pravo zaborava može iskoristiti svaki čovjek čiji se osobni podatci obrađuju. Zakon omogućava da osoba može u bilo kojem trenutku zatražiti zabranu obrade svojih osobnih podataka te njihovo brisanje.



Grafikon 16. Prikaz postotka ispitanika koji su upoznati sa Pravom zaborava

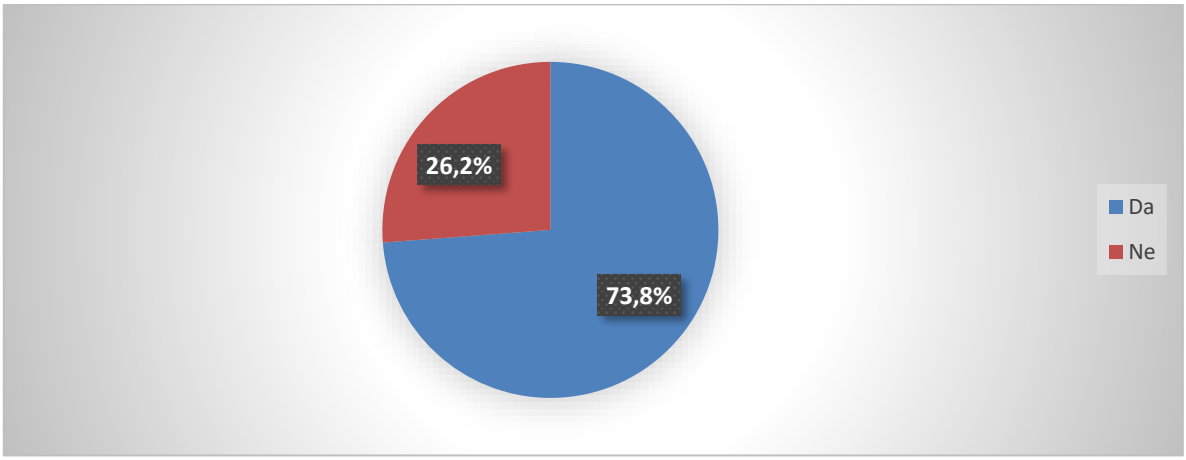
Registar ne zovi aktivan je od početka 2017. godine. U šest mjeseci postojanja čak 57,7% ispitanika nije upoznato s registrom niti ga koristi. 13,7% ispitanika koristi pravo na registar ne zovi. Svi stanovnici koji ne žele da ih se ne uznemirava telefonskim prodajama ili telefonskim anketama trebaju se samo registrirati u registru

ne zovi. Ukoliko netko nazove osobu koja je u registru ne zovi podliježe novčanim kaznama kako je propisano zakonom.



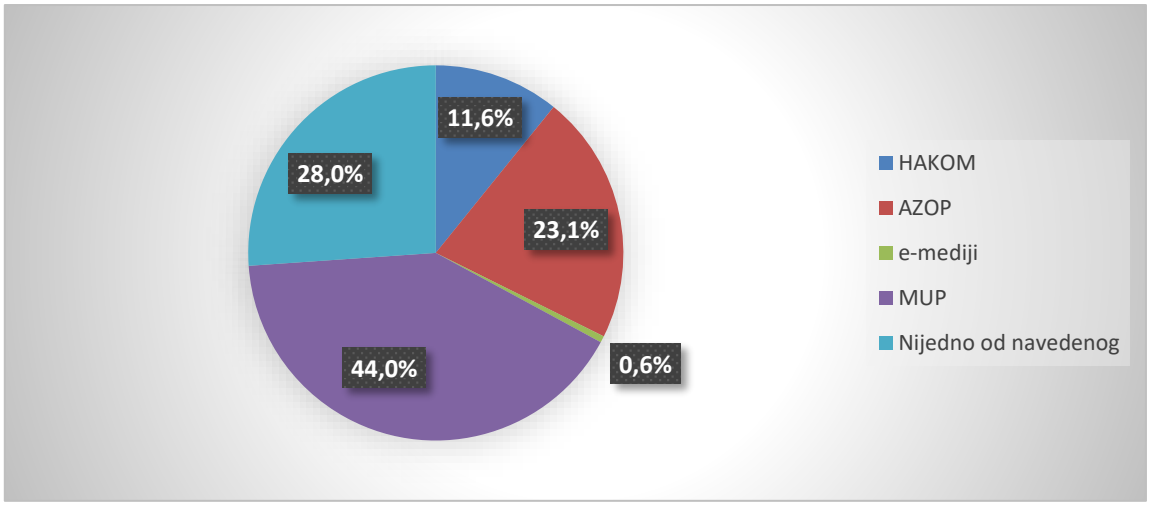
Grafikon 17. Odgovor na anketno pitanje "Koristite li registar ne zovi?"

Grafikon ispod prikazuje da 73,8% ispitanika zna da se njihovi podatci mogu obrađivati ukoliko su javno objavljeni. Pošto je anketu ispunilo najviše ljudi do 35 godina starosti, možemo zaključiti da mlađa generacija, koja objavljuje svoje podatke po društvenim mrežama, zna da ukoliko nešto objave to postaje javni podatak.



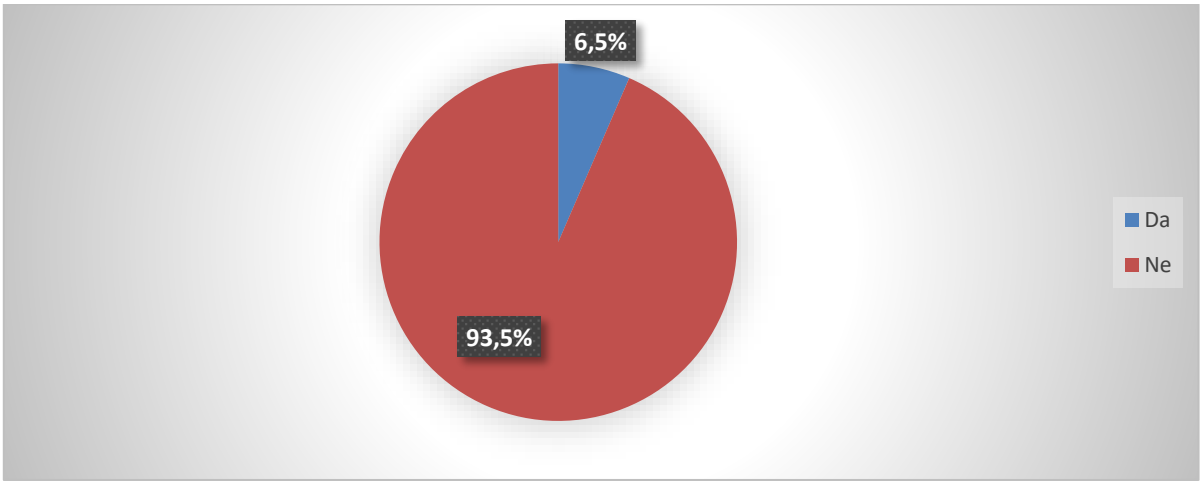
Grafikon 18. Odgovor na anketno pitanje "Znate li da se podatci smiju obrađivati ukoliko su javno objavljeni?"

Iz grafikona 19. vidimo da samo 23.1% ispitanika zna koja agencija vrši nadzor nad zaštitom osobnih podataka. Najveći broj ispitanika misli da Ministarstvo unutarnjih poslova nadzire zaštitu osobnih podataka, što nije točno. Agencija koja vrši nadzor zove se Agencija za zaštitu osobnih podataka.



Grafikon 19. Odgovor na anketno pitanje "Tko vrši nadzor nad zaštitom osobnih podataka?"

Grafikon 20. prikazuje koliko malo ljudi zna da se donose novi propisi i regulative po pitanju zaštite podataka. Samo 6,5% ispitanika je upoznato s novom regulativom, odnosno zna da se raspravlja o novim zakonima po pitanju zaštite podataka.



Grafikon 20. Prikaz koliko je ispitanika upoznato s promjenama koje se događaju u zemljama EU a odnose se na zaštitu

Iako su ispitanici uglavnom mladi ljudi ili zrele dobi, pretežno ženskog roda, posjeduju mobilni telefon i svakodnevno ga koriste, jedan manji dio i dalje ne zna što je osobni podatak, a svakodnevno objavljuju bezbroj slika, statusa te dijele razne lokacije na kojima se nalaze. Zabrinjavajući je podatak da dio istih ispitanika nije čuo za nove regulative i zakonske promjene koje se donese na području Europske unije,

a odnose na zaštitu osobnih podataka. Iz ankete se lako zaključuje kako ti ispitanici uopće nemaju dojam o stvarnim opasnostima kojima su izloženi svakodnevnim korištenjem tehnologije i društvenih mreža. Većina ispitanika je sigurna da Ministarstvo unutarnjih poslova brine o njihovim podatcima a samo mali broj njih zna da je to Agencija za zaštitu osobnih podataka. Mediji uz sve informacije koje pružaju ispitanicima bi trebali više pažnje posvetiti problemima koji nastaju zbog nepažnje i neznanja. Dobar dio informacija koje ispitanici znaju su saznali uglavnom putem TV-a, internetskih portala ili preko obavijesti operatora. Ispitanike bi trebalo češće obavještavati o promjena koje štite podatke iz njihovog života a i oni bi sami trebali više pažnje posvetiti takvim stvarima. Vrlo zabrinjavajući je podatak da samo 6,5 % stanovnika zna da se događaju promjene po pitanju zaštite osobnih podataka, a još uvijek manje od 30% ispitanika zna da postoji Agencija za zaštitu osobnih podataka.

8. Zaključak

Prilikom izrade diplomskog rada detaljno istraženo je područje zaštite osobnih podataka i odredbi Europske unije koje se odnose na zaštitu korisnika od raznih pokušaja prevare i krađe podataka kojima su korisnici izloženi svakodnevno a da većina njih nije ni svjesna opasnosti. Prema postojećem stanju lako je uočljiv trend rasta prijenosa osobnih podataka putem interneta pri raznim Internet kupovinama ili podjelom podatka na društvenim mrežama.

Kao rezultat uvođenja novih uredbi od strane Europske unije sve zemlje članice su dužne od 2016. godine omogućiti stanovnicima pravo na brisanje osobnih podataka, jasan i pozitivan pristanak na obradu osobnih podataka od strane ispitane osobe, pravo na prijenos podataka drugom voditelju obrade, obavješćivanje ispitanika o povredi osobnih podataka te uz gore navedeno još je potrebno osigurati da su pravila o privatnosti objašnjena jasnim i razumljivim jezikom.

Anketu su dobiveni rezultati u kojima se vidi da je najviše ispitanika mlađe od 35 godina. Spomenuta generacija gotovo svakodnevno objavljuje slike na internetu, dijeli lokacije na kojima se nalazi a vrlo malo zna o osobnim podatcima i o zaštiti podataka. Može se zaključiti da mlađa generacija nema interesa po pitanju edukacije o novim propisima koji se odnose na zaštitu osobnih podataka. Zabrinjavajući je podatak da samo 6,5% ispitanika zna da postoji nova Uredba, ali vrlo vjerojatno ni 3% ispitanika ne zna što se točno mijenja novom Uredbom. Sve članice Europske unije bi trebale putem medija educirati stanovništvo o novim pravilima koja se donose. Sve dok nećemo imati dovoljno educirano društvo, nećemo ni imati potrebnu zaštitu i sigurnost u modernom tehnološkom svijetu. Iz analize koja je napravljena u ovom radu može se zaključiti, kako nije problem u lošim tehnološkim zaštitama, ili sigurnosnim propustima nekih računalnih sustava, najveći problem je needuciranost stanovništva i njihova nezainteresiranost.

LITERATURA

1. Fakultet prometnih znanosti; Zakon o zaštiti osobnih podataka – Vojković G., 2016.:
    - http://e-student.fpz.hr/Predmeti/T/Telekomunikacijska_legislativa_i_standardizacija/Materijali/Osnove_zastite_osobnih_podataka.pdf (22.1.2017.)
2. Europski parlament Vama na usluzi - Zaštita osobnih podataka
    - http://www.europarl.europa.eu/atyourservice/hr/displayFtu.html?ftuId=FTU_5.12.8.html (25.1.2017.)
3. Zakon HR; Zakon o zaštiti osobnih podataka NN 103/03, 118/06, 41/08, 130/11, 106/12
    - http://www.zakon.hr/z/220/Zakon-o-za%C5%A1titi-osobnih-podataka (2.2.2017.)
4. Agencija za zaštitu osobnih podataka; Konvencija 108 Vijeća Europe,
    - http://www.azop.hr/images/dokumenti/168/konvencija_108_vijeca_europe.doc (5.2.2017.)
5. Agencija za zaštitu osobnih podataka; Direktiva 95/46/EZ,
    - http://www.azop.hr/images/dokumenti/168/direktiva_9546ez.doc (5.2.2017.)
6. Službeni list Europskih zajednica; Direktiva 2002/58/EZ EUROPSKOG PARLAMENTA I VIJEĆA od 12. srpnja 2002. o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija - Direktiva o privatnosti i elektroničkim komunikacijama
    - https://www.hakom.hr/UserDocsImages/2015/propisi_pravilnici_zakoni/uriCELEX%2032002L0058rid1.pdf (5.2.2017.)
7. Agencija za zaštitu osobnih podataka; Strateški plan AZOP-a za razdoblje 2017. - 2019. godine, Prosinac, 2016. godine
    - http://azop.hr/images/dokumenti/217/strateski-plan-azop.pdf (6.2.2017.)

8. Narodne Novine; Zakon o zaštiti osobnih podataka - ODBOR ZA ZAKONODAVSTVO HRVATSKOGA SABORA, Zagreb, 17. rujna 2012.
    - http://narodne-novine.nn.hr/clanci/sluzbeni/2012_09_106_2300.html (8.2.2017.)
9. Agencija za zaštitu osobnih podataka, Što je krađa identiteta?
    - http://azop.hr/aktualno/detaljnije/krada-identiteta-i-kako-se-zastititi (15.2.2017.)
10. SciTechBlog; Facebook fixes security bug in chat program, 2010.
    - http://scitech.blogs.cnn.com/2010/05/05/blog-finds-possible-security-flaw-in-facebook-chat/ (10.3.2017.)
11. Huffpost; Facebook Flaw Exposes Your Chats - Lets Friends See Your Conversations (VIDEO) 2010.,
    - http://www.huffingtonpost.com/2010/05/05/facebook-flaw-exposes-you_n_564126.html (12.3.2017.)
12. Google Launches Self-Service Advertising Program; Google AdWords Launch Press Release
    - http://googlepress.blogspot.hr/2000/10/google-launches-self-service.html (03.7.2017.)
13. Odaberite kako želite dosezati klijente; Display Ads, Video Ads, Search Ads & App Ads - Google AdWords
    - https://adwords.google.com/home/how-it-works/#?modal_active=none (22.7.2017.)
14. Agencija za zaštitu osobnih podataka; Strateški planovi,
    - http://azop.hr/info-servis/detaljnije/strateski-planovi (03.7.2017.)
15. Dragičević, D.: Pravna informatika i pravo informacijskih tehnologija, Narodne Novine, Zagreb 2015.
16. Brezek, M.: Pravo na osobnost, Nakladni zavod Matice Hrvatske, Zagreb 1998.
17. Westin, A. F.: Privacy and Freedom, Atheneum, New York 1967., str.7.

18. Michael, J.: Privacy and human Rights: An International and Comparative Study, with Special Reference to Development sin Information Tehnology,. UNESCO, Darmouth 1994., str.1.
19. Reidenberg, J.R.: Restorng Americans Privacy in Electronical Commerce, 14 Berkeley Tech. L.J. (1999)
20. Art.29 WP, Working document on determining the international application of EU dana protection law personal dana processing on the Internet by non-EU based web sites, WP 56, 30.5.2002, str. 9-12.
21. Razvoj računala kroz povijest,
    - http://www.zbrdazdola.com/infobible/infobible/razvoj_racunala_kroz_povijest.htm (22.7.2017.)
22. CARNet; Napredne tehnike socijalnog inženjeringa NCERT-PUBDOC-2010-02-292
    - http://www.cert.hr/sites/default/files/NCERT-PUBDOC-2010-02-292.pdf (22.7.2017.)
23. Tutorialspoint; Computer Fundamentals, Computer – Generations
    - https://www.tutorialspoint.com/computer_fundamentals/computer_generations.htm (22.7.2017.)
24. Znanost, Hrvatski popularno-znanstveni portal; Učeći od mozga: informatički znanstvenici razvijaju novu generaciju neuro-računala
    - https://geek.hr/znanost/clanak/uceci-od-mozga-informaticki-znanstvenici-razvijaju-novu-generaciju-neuro-racunala/ (22.7.2017.)
25. First Draft of a Report on the EDVAC by John von Neumann, Moore School of Electrical Engineering University of Pennsylvania, 1945.
    - http://www.virtualtravelog.net/wp/wp-content/media/2003-08-TheFirstDraft.pdf (22.8.2017.)
26. F. Faggin, M. Shima, M.E. Hoff, Jr., H. Feeney, S. Mazor: "The MCS-4—An LSI micro computer system". IEEE '72 Region Six Conference. Reprinted on pp. 6–32 to 6–37 of The Intel Memory Design Handbook: 1973.
27. "3rd Generation Microprocessor" (PDF). Microcomputer Digest. Cupertino, CA: Microcomputer Associates. 2 (2): 1–3. 1975.

28. "Microprocessor Hall of Fame". Intel.
    - https://www.landley.net/history/mirror/collate/hof_main.htm (20.06.2017.)
29. Intel brochure – 11/91. "Directory page for Top500 lists. Result for each list since June 1993". Top500.org
30. Article 29 Dana Protection Working Party, Opinion 2/2010 on online behavioural advertising, 00909/10/EN, WP 171, 22.06.2010.
31. PC ADVISOR; Intel Core i9 release date, features, specs,
    - http://www.techadvisor.co.uk/new-product/pc-upgrades/intel-core-i9-release-date-features-specs-3590751/ (25.08.2017.)
32. 16 th International Scientific Conference on Economic and Social Development – "The Legal Challenges of Modern World"
    - https://www.esd-conference.com/upload/book_of_proceedings/esd_Book_of_Proceedings_Split_2016_Online.pdf (26.8.2017.)
33. Drahos, P., Braithwaite, P. J., Information Feudalism: Who Owns the Knowledge Economy?, Earthscan, 2002
34. General Data Protection Regulation- GDPR, (2016), OJ L 119, 4.5.2016, p. 1–88 (2016), Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, 10.08.2016.
    - http://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:32016R0679&from=EN://eurlex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:T OC (21.06.2017.)
35. Konferencija o informacijskoj sigurnosti u Hrvatskoj FSec 2017, GDPR – uredba o zaštiti osobnih podataka, Varaždin FSec, 7.9.2017.
36. Boban M., Konferencija o informacijskoj sigurnosti u Hrvatskoj FSec 2017, GDPR – uredba o zaštiti osobnih podataka, Varaždin FSec, 7.9.2017.

37. Vojković G., Konferencija o informacijskoj sigurnosti u Hrvatskoj FSec 2017, GDPR – uredba o zaštiti osobnih podataka, Varaždin FSec, 7.9.2017.
38. Michael, J., Privacy and human Rights: An International and Comparative Study, with Special Reference to Development sin Information Tehnology,. UNESCO, Darmouth 1994., str.1.
39. 1. STANOVNIŠTVO PREMA STAROSTI I SPOLU PO NASELJIMA, POPIS 2011.
    - http://www.dzs.hr/Hrv/censuses/census2011/results/htm/H01_01_01/H01_01_01.html (01.09.2017.)
40. Raosoft; Simple size calculator;
    - http://www.raosoft.com/samplesize.html

POPIS TABLICA

POPIS GRAFIKONA

PRILOG I

PITANJA ANKETNOG UPITNIKA:

1. Vaš spol je:

- Muško
- Žensko

2. Vaša dobna skupina je:

- Između 18-24 godina
- Između 25-35 godina
- Između 36-45 godina
- Između 46-55 godina
- Između 55-65 godina
- Iznad 65 godina

3. Vaše mjesto stanovanja je:

- Naselje do 20.000 stanovnika
- Naselje od 20.001 do 50.000 stanovnika
- Naselje od 50.001 - 100.000 stanovnika
- Naselje od 100.001- 200.000 stanovnika
- Naselje iznad 200.001 stanovnika

4. Završeno obrazovanje:

- Osnovno obrazovanje

- Srednjoškolsko obrazovanje
- Sveučilišni diplomski studij
- Poslijediplomski znanstveni magistarski studij/doktorat

5. Vaša obitelj:

- Samac
- Obitelj s 2 člana
- Obitelj s 3 člana
- Obitelj s 4 i više članova

6. Vaše zanimanje:

- Učenik
- Student
- Zaposlen
- Nezaposlen
- U mirovini

7. Vrsta mobilnog uređaja koji koristite:

- Klasični mobitel
- Pametni telefon (smartphone)

8. Mailove putem mobilnog uređaja pregledavam:

- Više puta dnevno
- Svaki dan

- Jednom tjedno
- Jednom mjesečno
- Ne gledam preko mobitela

9. Uređaj putem kojeg se registrirate na internet stranicama…

- Mobilni uređaj
- Tablet
- Računalo
- Ne registriram se na internet stranicama

10. Produljivanje ugovorne obveze sa teleoperaterima na daljinu…

- Prihvaćam putem telefona
- Prihvaćam putem mobilnog uređaja
- Prihvaćam putem interneta (webshop)
- Prihvaćam putem maila
- Ne produljujem ugovore na daljinu - (idem u poslovnicu)

11. Osobni podatak je:

- Ime i prezime
- OIB
- Adresa
- Datum rođenja
- Konfekcijski broj obuće
- Grad stanovanja

- Naziv završene osnovne škole
- Ime bračnog partera/partnerice

12. Kada Vas netko zove na telefon i predstavi se kao telekom operater, vjerujete li da se ne predstavlja lažno:

- Da
- Ne

13. Kako provjerite dali je osoba koja Vas je nazvala stvarno zaposlenik telekom operatera:

- Tražite puno ime i prezime te osobe
- Zovete službu za korisnike i tražite navedenu osobu prema imenu i prezimenu
- Tražite potvrdu mailom
- Ništa od navedenog

14. Šaljete li mailom kopiju osobne iskaznice na mail kao potvrdu svog identiteta:

- Da
- Ne

15. Znate li kome ste dužni davati osobne podatke:

- Da
- Ne

16. Tko smije prikupljati i obrađivati Vaše osobne podatke bez vašeg znanja:

- Policija

- Pošta
- Telekom operatori
- Anketari
- Banke
- Nitko

17. Jeste li upoznati s pravom zaborava prikupljenih podataka:

- Da
- Ne

18. Koristite li pravo na registar "ne zovi":

- Da
- Ne
- Nisam upoznat s tim registrom

19. Jeste li upoznati s informacijom da se vaši podatci mogu obrađivati ukoliko ste ih javno objavili:

- Da
- Ne

20. Znate li da je svaka osoba koja Vas traži osobne podatke dužna navesti točan razlog zbog kojeg prikuplja podatke:

- Da
- Ne

21. Znate li koja agencija vrši nadzor nad zaštitom Vaših osobnih podataka:

- HAKOM
- AZOP
- e – mediji
- MUP
- Nijedno od navedenog

22. Jeste li upoznati s novim promjenama koje se događaju u zemljama EU a odnose se na zaštitu osobnih podataka(Nova uredba o zaštiti osobnih podataka):

- Da
- Ne

METAPODACI

Naslov rada: Zaštita osobnih podataka s osvrtom na Opću uredba o zaštiti podataka

Autor: Mislav Matusina univ. bacc. ing. traff.

Mentor: doc. dr. sc. Goran Vojković

Naslov na drugom jeziku (engleski):

Personal data protection with review to General Data Protection Regulation

Povjerenstvo za obranu:

- prof. dr. sc. Dragan Peraković predsjednik
- doc. dr. sc. Goran Vojković mentor
- doc. dr. sc. Štefica Mrvelj član
- prof. dr. sc. Ivan Gregurević zamjena

Ustanova koja je dodijelila akademski stupanj: Fakultet prometnih znanosti Sveučilišta u Zagrebu

Zavod: Zavod za informacijsko komunikacijski promet

Vrsta studija: Sveučilišni

Naziv studijskog programa: Promet

Stupanj: Diplomski

Akademski naziv: mag. ing. traff

Datum obrane završnog rada:_____

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOST

Izjavljujem i svojim potpisom potvrđujem da je ovaj diplomski rad isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu, a što pokazuju korištene bilješke i bibliografija. Izjavljujem da nijedan dio rada nije napisan na nedozvoljen način, odnosno da je prepisan iz necitiranog rada, te da nijedan dio rada ne krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu diplomskog rada pod naslovom: „Zaštita osobnih podataka s osvrtom na Opću uredbu o zaštiti podataka“ na internetskim stranicama i repozitoriju Fakulteta prometnih znanosti, Digitalnom akademskom repozitoriju (DAR) pri Nacionalnoj i sveučilišnoj knjižnici u Zagrebu.

U Zagrebu,_____

Student:

_____